
CONFIGURATION MIGRATION TOOL

# FortiConverter User Guide

**VERSION 5.4.1**

**FORTINET DOCUMENT LIBRARY**

http://docs.fortinet.com

**FORTINET VIDEO GUIDE**

http://video.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

**FORTIGATE COOKBOOK**

http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**

http://www.fortinet.com/training

**FORTIGUARD CENTER**

http://www.fortiguard.com

**FORTICAST**

http://forticast.fortinet.com

**CLI REFERENCE**

http://cli.fortinet.com

**END USER LICENSE AGREEMENT**

http://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**

Email: techdocs@fortinet.com

April 10, 2018

FortiConverter 5.4.1 User Guide

1st Edition

# TABLE OF CONTENTS

# Introduction

This document shows how to install and use FortiConverter.

FortiConverter is designed to help you migrate your network to Fortinet network security solutions, significantly reducing workload and minimizing errors. FortiConverter translates configuration files from other vendors' firewall products into a valid FortiGate or FortiManager configuration file. Because the output uses command line syntax, it can either be uploaded as a configuration file or piped to the CLI.

For additional assistance, please contact fconvert_feedback@fortinet.com.

## Submitting configuration files and retrieving private builds via SCP

FortiConverter customers can securely submit firewall configuration files to Fortinet Engineering using Fortinet's SCP (Secure CoPy) service.

You can use the same service to retrieve private builds that fix conversion logic, if required.

Because this account has many restrictions, Fortinet recommends that you use a command-line SCP client to transfer files. For example, PSCP provides a suitable SCP client for Windows users.

### To upload a file

1. Create a zip archive with a name that is unique to your case (for example, your FortiConverter serial number).
2. Add your files to the zip archive, even if you have only one file to send.
3. Use your SCP client to connect to the secure server and upload the file using the following settings:

| | |
|---|---|
| **Server** | ftp.apsecure.com |
| **Port** | 2222 |
| **User** | fcon-incoming |
| **Password** | incoming |

For example, for PSCP:

```
.\pscp.exe -P 2222 fcon0123456789.zip fcon-incoming@ftp.apsecure.com:.
```

### To download a file

1. Obtain the name of the file to retrieve from Fortinet Engineering (for example, `fcon-build-0123456789.exe`).
2. Use your SCP client to connect to the secure server and download the file using the following settings:

| | |
|---|---|
| **Server** | ftp.apsecure.com |

| | |
|---|---|
| **Port** | 2222 |
| **User** | fcon-outgoing |
| **Password** | outgoing |

For example, for PSCP:

```
.\pscp.exe -P 2222 fcon-outgoing@ftp.apsecure.com:fcon-build-0123456789.exe .
```

# Supported vendors & configuration objects

FortiConverter can translate configurations from the following vendors and models.

In some cases, FortiConverter cannot translate some parts of the configuration because of dependencies or unsupported syntax and you must manually convert them.

If the number of objects exceeds the maximum valid length for FortiGate or FortiManager, FortiConverter trims them.

FortiConverter comes with two different applications, each capable of a different set of conversions. The Converter Application column shows which FortiConverter application to use for each conversion.

## Alcatel-Lucent

| Models | Converter Application | Versions | Convertible objects |
|---|---|---|---|
| **Brick** | Legacy Application | ALSMS v9.x | Addresses & Address Books<br>Interfaces (physical, logical, loopback, PPPoE)<br>Partitions<br>Services & Service Books<br>Static routes<br>Zone rule set |

## Check Point

| Models | Converter Application | Versions | Convertible objects |
|---|---|---|---|
| **SmartCenter** | Legacy Application | NG FP1 (4.0) to NGX R80 | Addresses & Address Groups<br>Interfaces (Physical, Logical, Loopback, PPPoE)<br>Local Users & Groups<br>NAT (Automatic & Rule)<br>Negate Cell<br>Policies (rulebases.fws)<br>RADIUS, TACACS+, & LDAP<br>Rules<br>Schedules<br>Services & Service Groups<br>Static routes<br>VPN (IPSec) |
| **Provider-1** | Legacy Application | NGX R65 to R80 | |

## Cisco

| Models | Converter Application | Versions | Convertible objects |
|---|---|---|---|
| **PIX** | New Application | 4.x to pre-8.3, 8.3 and later, 9.x | ACLs<br>Addresses & Address Groups<br>DHCP Servers<br>DNS Servers<br>Interfaces (Physical, Logical, Loopback, PPPoE, Tunnel)<br>IP Pools<br>Local Users & Groups<br>NAT (including Object NAT and Double NAT)<br>RADIUS, TACACS+, & LDAP<br>Services & Service Groups<br>Static Routes<br>Time Ranges<br>VPN (IPSec, PPTP/L2TP, EZVPN) |
| **ASA** | New Application | | |
| **FWSM** | New Application | | |
| **IOS** | Legacy Application | 10.x to 12.x<br>15.x | |
| **IOS XR** | Legacy Application | 4.x, 5.x, 6.x | Addresses & Address Groups & FQDNs Interfaces<br>IP Pools<br>Policies<br>Services & Service Groups<br>Static Routes |
| **Nexus** | Legacy Application | 5.2, 6.x, 7.x | |

### Juniper

| Models | Converter Application | Versions | Convertible objects |
|---|---|---|---|
| **SSG/ISG** | Legacy Application | ScreenOS 5.x, 6.x | Addresses & Address Groups & FQDNs<br>DHCP Servers & Clients & Relays<br>Interfaces (Physical, Logical, Loopback, PPPoE, Tunnel)<br>Static Routes<br>Services & Service Groups<br>Policies<br>VIPs/MIPs<br>NAT<br>IP Pools<br>VPN (IPSec, PPTP/L2TP)<br>Local Users & Groups<br>RADIUS & LDAP<br>Zones |
| **SRX** | Legacy Application | Junos OS 10.x to 12.x | Addresses & Address Groups & FQDNs<br>DHCP Servers & Client & Relay<br>Interfaces (Physical, Logical, Loopback, PPPoE, Tunnel)<br>IP Pools<br>Local Users & Groups<br>NAT<br>Policies<br>RADIUS & LDAP<br>Services & Service Groups<br>Static Routes<br>VIPs/MIPs<br>VPN (IPSec, PPTP/L2TP)<br>Zones |
| **MX** | Legacy Application | Juno OS 10.x to 12.x | Addresses & Address Groups & FQDNs<br>Interfaces<br>IP Pools<br>Policies<br>Services & Service Groups<br>Static Routes |

### McAfee

| Models | Converter Application | Versions | Convertible objects |
|---|---|---|---|
| **Sidewinder** | Legacy Application | 7.x, 8.x | Addresses & Address Groups & FQDNs<br>Interfaces<br>IP Pools<br>Policies<br>Services & Service Groups<br>Static Routes |
| **StoneSoft** | Legacy Application | 5.7 | Addresses & Address Groups<br>Interfaces<br>Policies<br>Services & Service Groups<br>Static Routes<br>NAT (Static Source NAT, Dynamic Source NAT, Destination NAT) |

### Palo Alto Networks

| Models | Converter Application | Versions | Convertible objects |
|---|---|---|---|
| **PA** | Legacy Application | PAN-OS 1.x to 6.x | Addresses & Address Groups & FQDNs<br>Interfaces<br>Local Users & Groups<br>NAT (partial)<br>Policies<br>Schedules<br>Static Routes<br>Services & Service Groups<br>Zones |

### SonicWall

| Models | Converter Application | Versions | Convertible objects |
|---|---|---|---|
| **NSA Series** | Legacy Application | SonicOS Enhanced 5.x | Addresses & Address Groups & FQDNs<br>DHCP Servers & Clients & Relays<br>Interfaces (Physical, Logical, Loopback, PPPoE)<br>Local Users & Groups<br>NAT<br>Policies<br>Schedules<br>Services & Service Groups<br>Static Routes<br>Zones |

### Tipping Point

| Models | Converter Application | Versions | Convertible objects |
|---|---|---|---|
| **IPS** | Legacy Application | 4.5 | Addresses & Address Groups<br>Policies<br>Services & Service Groups |

## General limitations

FortiConverter is a migration tool, not a migration service. It is designed to be used as part of a properly planned migration process.

#### Supported FortiOS conversions

FortiConverter supports conversions from other vendors to FortiOS 5.4 and 5.6 only.

#### Creating final configurations

While FortiConverter significantly shortens the conversion process, a final, useable configuration requires you to review and audit the FortiConverter output conversion. FortiConverter's tuning capability can help with the review and audit process.

While you can use FortiConverter's tuning capability to review and fix errors in the conversion, it is not designed to perform significant reconfiguration.

#### Incomplete routing information

In some cases, not all the routing information that FortiConverter requires to make a decision about a policy interface is available. In these cases, it uses the 'any' interface.

#### Double NAT

For Check Point conversions, the FortiConverter conversion engine uses a manual rule to convert configurations that apply source NAT and destination NAT to the same policy (called double NAT).

For all other conversions, FortiConverter NAT merge does not support double NAT. Instead, FortiConverter applies source NAT in the conversion and you complete the configuration by using the tuning page to manually apply destination NAT.

#### IPsec support

FortiConverter converts IPsec configurations to route-based or policy-based IPsec depending on which one the source configuration is closest to.Users can enable Route-based IPSec for Cisco ASA, PIX,FWSM, and Check Point conversions.

**FortiGate conversion**

FortiConverter firewall configuration migration tool is primarily for third-party firewall configuration migration to FortiOS—for routing, firewall, NAT, and VPN policies and objects.

## Licensing

With the trial version of FortiConverter, you can complete a conversion and view the results in the tuning page. CLI and API output are disabled until you upload the full license.

After you purchase and upload a license, FortiConverter is unlocked and full functionality is enabled for all supported vendors. Your paid license entitles you to any new versions of FortiConverter that Fortinet releases until the license expires, as well as direct engineering support.

FortiConverter 5.4.1 features a new browser/server based application in addition to the legacy application. Both the new application and legacy application use the same license key and should be installed on the same host.

FortiConverter requires an Internet connection to verify its license. You can use the software for up to 30 days without validating the license online, and you can configure FortiConverter to contact the licensing server via a web proxy.

For more information, see "Uploading the license" on page 19

## System requirements

FortiConverter requires one of the following operating systems:

- Microsoft Windows 10
- Microsoft Windows 8 (32-bit or 64-bit)
- Microsoft Windows 7 (32-bit or 64-bit)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012

In addition, FortiConverter requires .NET Framework 4.0. If it is not already installed on your computer, the FortiConverter installer prompts you to download and install it.

A web browser is required to view conversion reports.

An Internet connection is required to verify the software license.

# What's new

The following list contains new features and enhancements in FortiConverter 5.4.

**FortiConverter 5.4**

- **New application**—FortiConverter now features a new application for Cisco ASA, PIX, and FWSM conversions. These conversions have been removed from the legacy application.
- **FortiGate configuration viewer**—The new FortiConverter application features a configuration viewer for viewing older FortiGate configurations. The FortiGate to FortiGate configuration option has been removed.
- **Trend Micro Tipping Point**—FortiConverter now supports conversion from Trend Micro Tipping Point IPS 4.5 to FortiOS.
- **McAfee Stonesoft**—FortiConverter now supports conversion from Stonesoft 5.7 to FortiOS.
- **Copy to CLI**—Copy to CLI is now available for all conversions. This feature allows you to select conversion-dataset objects from the GUI (tuning) and copy or save their CLI configuration. For the FortiOS viewer, the Copy to CLI output can optionally be translated to a later FortiOS syntax.
- **FortiConverter icon change**—The FortiConverter icon now directly opens the FortiConverter home page.
- **Version info warning message**—FortiConverter now displays a warning message if the firmware version info of the configuration file cannot be found.
- **Output file download**—Conversion output files can now be downloaded from the home page.

# Installation

## Installing the software

To download the FortiConverter installer from the Fortinet Technical Support website, go to:

https://support.fortinet.com

### To install the legacy FortiConverter application

1. Double-click the FortiConverter installer executable (.exe).

   If your computer does not have Microsoft .NET Framework 4.0, you are prompted to install it.

2. To proceed with the installation, click **Yes** and then download the software framework from Microsoft's web site.
3. To continue the installation, read the license agreement, select **I accept the terms of the License Agreement**, and then click **Next**.
4. If you want to install the program in a location that is different from the default one, click **Browse** and select the directory.
5. Click **Next**.
6. Select the Start Menu folder that you want to add the program shortcuts to, and then click **Install**.
7. Click **Finish** to exit the FortiConverter installer.

### To install the new FortiConverter application

If you have previously installed an **interim** version of the **new** FortiConverter application, you must safely remove it first before installing the latest version.

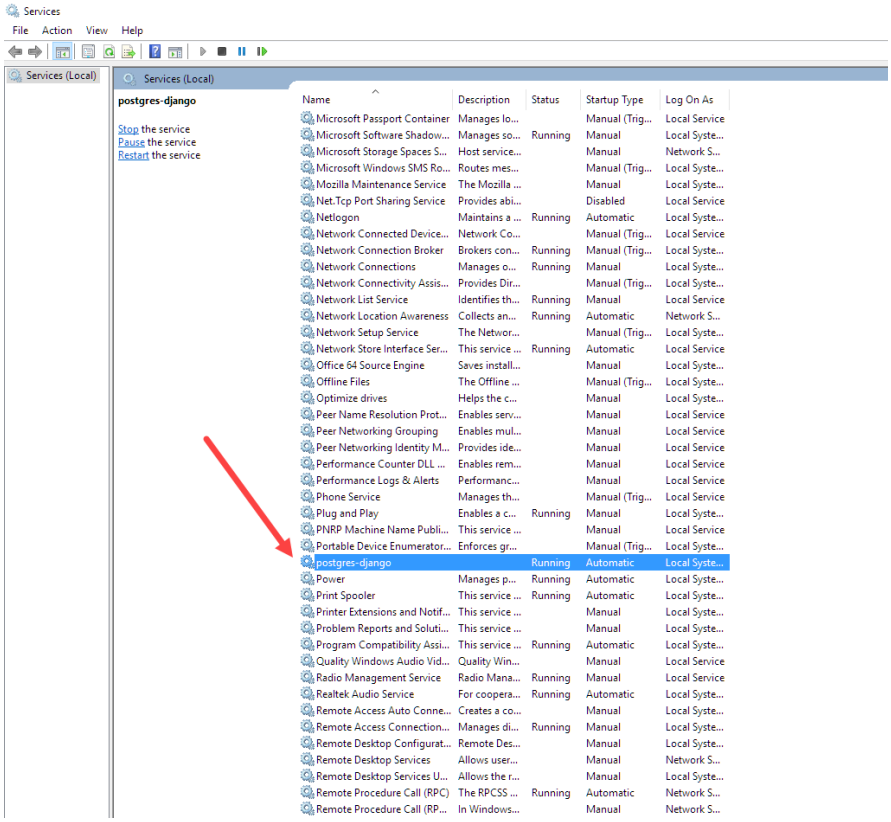
#### To safely remove a previous version of the new application

If this is your first time downloading the **new** FortiConverter application, skip this section.

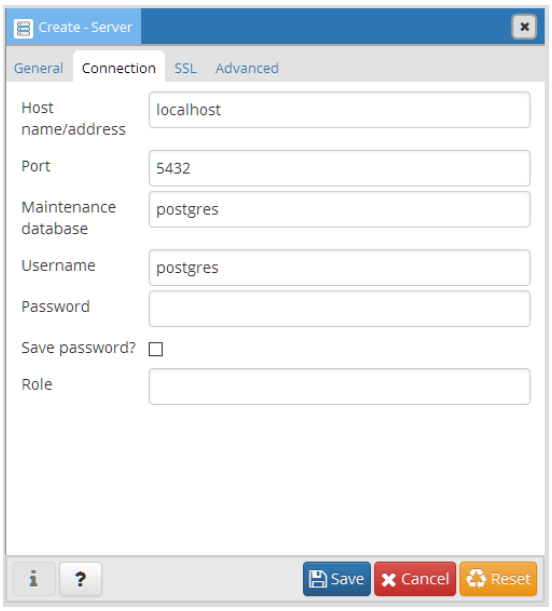
If your previous version is a General Availability (GA) version of FortiConverter, and you are upgrading to another GA version, this step is not necessary. Skip this section.

This procedure will delete all conversion data. Please save or back up all necessary conversions before continuing.

1. Stop the FortiConverter program.
2. Restart your local PostgreSQL database service.
   a. Open your Services desktop application.
   b. Right-click the service name **postgres-django**, and select **Restart**.



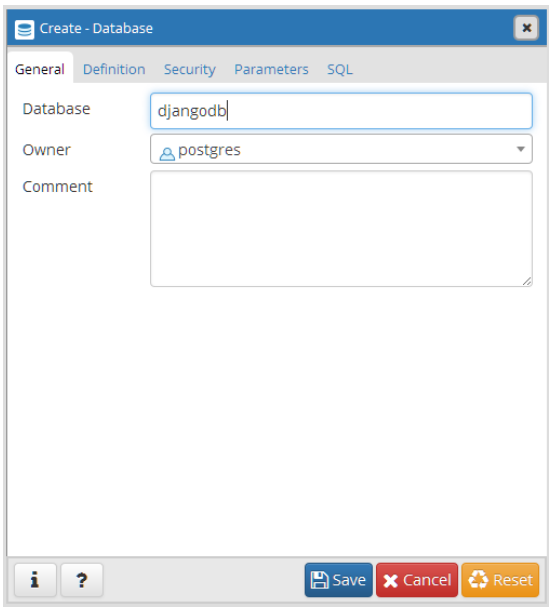

3. Install the latest version of pgAdmin 4, which can be downloaded at https://www.pgadmin.org/.
4. Using pgAdmin 4, create a server record.
   a. Go to **Object > Create > Server**.
5. Set both the username and password to "postgres".




6. Open the newly created service record, right-click the database "djangodb", and select **Delete/Drop**.
7. Click **OK**.
8. If you receive the error message: "there is 1 other session xxx", terminate all other existing external connections, except for the connection from pgAdmin 4.
    a. Make sure FortiConverter has been stopped.
    b. Click on the "djangodb" database.
    c. Go to **Tools > Query Tool**.
    d. Enter the following PSQL script, then click **Execute**.

```
SELECT
   pg_terminate_backend(pid)
FROM
   pg_stat_activity
WHERE
   -- don't kill my own connection!
   pid <> pg_backend_pid()
   -- don't kill the connections to other databases
   AND datname = 'djangodb';
```

9. Restart the pgAdmin 4 tool, and drop "djangodb" again, if available.
10. Re-create a database with the name "djangodb" by going to **Object > Create > Database** .
11. Click **Save**.




12. Delete all existing conversion folders to avoid a name conflict.
    Conversions are, by default, stored at `C:\Users\<UserName>\AppData\Roaming\Fortinet\FortiConverter\conversions`.
13. Uninstall the program.
14. Delete all remaining files and folders in the FortiConverter folder, located at `C:\Program Files\Fortinet\FortiConverter`.

**To install the latest version of the new application**

1. Double-click the FortiConverter installer executable (.py.exe).
2. To proceed with the installation, click **Yes** and then download the software framework from Microsoft's web site.
3. Click **Next**.
4. To continue the installation, read the license agreement, select **I accept the terms of the License Agreement**, and then click **Next**.
5. If you want to install the program in a location that is different from the default one, click **Browse** and select the directory.
6. Click **Next**.
7. Click **Install**.
8. Click **Finish** to exit the FortiConverter installer.

## Uploading the license

By default, FortiConverter is installed with a limited trial license. If you have purchased an full license, upload it to unlock the complete feature set.

To purchase a license, use your usual Fortinet sales channel.

For other licensing issues, see "Licensing" on page 135 for more information.

If you have already activated a license for the legacy FortiConverter application on your device, the new application will automatically use that license when it is installed.

## To activate the license

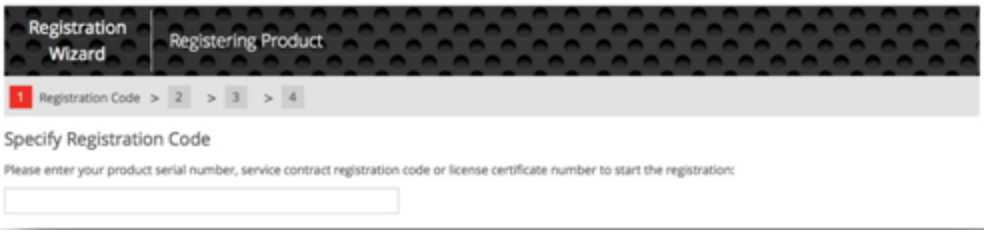
### Legacy application

1. To start FortiConverter, double-click its shortcut.
2. On the home page, click **More**.
3. Click **About FortiConverter**.
4. On the License tab, copy the **Hardware ID** value to the clipboard.
5. Ensure you have purchased a license, then sign in to the Fortinet Technical Support web site at the following location:

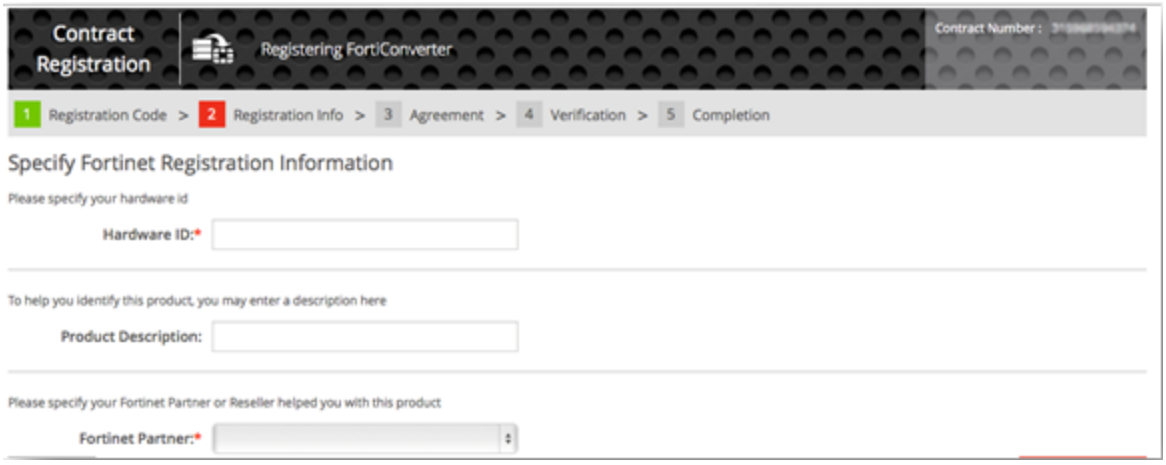
   https://support.fortinet.com/

   Registration uses a simple, four-step wizard that is commonly used for many Fortinet products.

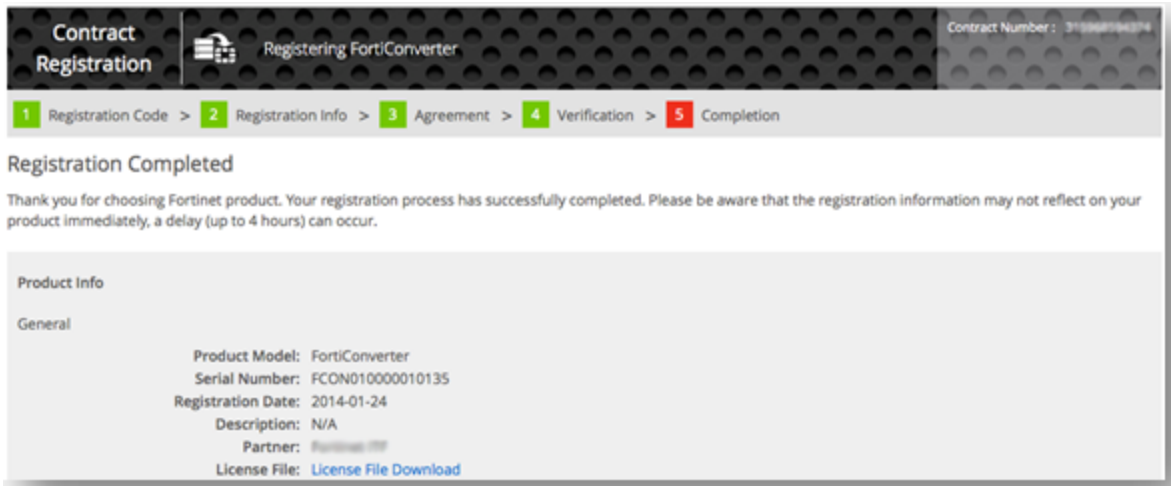
6. On the first page of the wizard, enter the registration code you received when you purchased your FortiConverter product.




7. For step 2 of the registration wizard, enter the **Hardware ID** you copied earlier, an optional description, and select the name of your Fortinet partner from the list.




8. After you agree to the license terms, the final page of the wizard (step 5) allows you to download the license file (.lic file).




9. In FortiConverter, on the **License** tab, click **Select** and navigate to the .lic file to select it.

10. Click **Activate**.

    FortiConverter validates the license file and changes your **Activation Status** from **Trial** to **Activate**.

    Your license is valid for all FortiConverter software updates released until the date specified by **License Expiry Date**.

    After the license is activated, to access the expiry information, go to the **License** tab.

### New application

1. To start FortiConverter, double-click its shortcut.
2. Click **License**.

3. Click the icon next to License File.
4. Select the license file, then click **Open**.

### License validation via web proxy

You can configure FortiConverter to use an explicit (non-transparent) web proxy server to connect to Fortinet's online licensing servers.

FortiConverter connects to the proxy using the HTTP CONNECT method, as described in RFC 2616.

1. On the home page, click **More**.
2. Click **About FortiConverter**.
3. On the Proxy tab, select **Enable Proxy** and then specify the IP address and the port of the web proxy to use.
4. Click **Apply**.

## Enabling remote connections—new application

The new FortiConverter is designed as a web application. The application (FortiConverter.py) should be run with Administrator privileges because it reads and writes data from/to high privilege directories. For security concerns, the default configuration only allows connections from users on the localhost.

### To enable remote access to the web application:

1. Run notepad.exe as an administrator and open the `start.bat` file located in the directory `C:\Program Files\Fortinet\FortiConverter\`.
2. Append string `0.0.0.0:<port_num>` after the keyword `runserver`. The port number used by default is 8000.

   For example:

   ```
   call "%install_dir%\Python36\python.exe" manage.py runserver 0.0.0.0:8000 --insecure
   ```
3. Run notepad.exe as an administrator and open `C:\Program Files\Fortinet\FortiConverter\converter\backend\mysite\mysite\settings.py`
4. Add the wildcard IP address `'*'` (match ANY) into allowed ALLOWED_HOSTS.

   For example:

   ```
   ALLOWED_HOSTS = [
      'localhost',
      '127.0.0.1',
      '*',
   ]
   ```

# Check Point conversions

## Check Point differences

### General

- FortiGate's `set allowaccess` command for interfaces does not exist on Check Point. Because FortiGate requires this setting, FortiConverter enables all services for interfaces by default.
- The interface "Lead to Internet" is a default static route on FortiGate.
- FortiConverter supports Traditional Mode and Simplified Mode IPSec.

### Schedule configuration

FortiConverter converts "Day in month" time schedules to FortiGate one-time schedules. It converts "Day in week" and "None" schedules to recurring schedules.

You assign a year range for the "Day in month" schedule. If the specified day does not exist for a certain month, FortiConverter does not generate the one-time schedule for that month.

### NAT and policy configuration

FortiConverter supports the conversion of the following NAT types:

- Hide NAT
- Static NAT
- Manual NAT

FortiConverter does not convert NAT global properties.

### VPN configuration

Check Point does not configure VPN within a firewall rule. When FortiConverter converts the configuration to FortiGate, it generates several VPN policies from non-"Lead to Internet" interfaces to the "Lead to Internet" (default route) interface.

After FortiConverter converts the VPN configuration, the VPN policy's destination interface refers to the "Lead to Internet" interface. If you changed the default route's egress interface, you may need to update the VPN/Policy configuration manually.

FortiConverter can support VPN IPSec policies configured in both Traditional Mode and Simplified Mode. However, FortiConverter can only convert one mode at a time. If encrypted rules are detected, FortiConverter will default to Traditional Mode conversion.

To convert Traditional Mode policies to Simplified Mode policies, use the Check Point Security Policy Converter Wizard. This can be found by clicking **Policy > Convert to > Simplified VPN** from the Check Point SmartDashboard.

FortiConverter can detect and convert meshed and star VPN topologies in Simplified form.

### Service objects

Unlike FortiGate service objects, Check Point service objects have a protocol type attribute. FortiGate uses a session helper object to provide the same functionality as the service objects with a protocol type attribute.

## Downloading the source configuration files

Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed.

To acquire the configuration, download the following files. In most cases, you download the object and policy definitions from the management system:

- Object definitions — 'objects_5_0.C' (Check Point NG/NGX) or 'objects.C' (Check Point 4.x) contain the firewall's object definitions. To convert from Provider-1, 'mcss.C' contains the MDS hierarchy files.
- Policy and rule definitions — '*.w' or 'rulebases_5_0.fws'. The file name is <rule>.W (default Standard.W). or rulebases_5_0.fws. They are located in the directory "[SmartCenter] : $FWDIR/conf".
- Route information (optional) — Helps FortiConverter to correctly interpret the network topology being converted. To get this data, enter the `route print` command on the firewall node, and then copy and paste the output into a plain text file. Codes in the output indicate if the route is a directly connected interface, a host route, a network route, and so on. The output varies by the platform.
- User and user groups file (optional) — fwauth.NDBx

Ensure the configuration is in a text format (for example, in plain text or XML). FortiConverter cannot use binary files.

| File | File name | Path |
|---|---|---|
| Object definitions | objects_5_0.C (Checkpoint NG/NGX)<br><br>objects.C (Checkpoint 4.x_) | $FWDIR/conf |
| | mcss.C (Provider-1) | $MDSDIR/conf/mdsdb |
| Policy and Rule definitions | rulebase_5_0.fws<br><br>[package name].W | $FWDIR/conf |
| Route information | NA | Save output of route print command from firewall |

| File | File name | Path |
|---|---|---|
| User and User Group file | fwauth.NDBx | $FWDIR/conf/<br>or<br>$FWDIR/database/ |

# Running the Check Point conversion

## Check Point conversion wizard

The administrator password is **not** set on the new configuration.

Trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

The pages that the Check Point conversion wizard displays depend on whether your source configuration is SmartCenter or Provider-1.

Because Provider-1 uses global and device-level virtual domains that are similar to FortiManager ADOMs, you convert Provider-1 configurations to policy packages and objects for your source firewalls in the FortiManager Policy & Objects database. You can only select FortiManager as the output format on the Start Options page.

### Start Options

| Setting | Description |
|---|---|
| **Model** | Select the source Check Point model. |
| **Output Format** | Select the appropriate output for your target Fortinet device.<br>You can convert Provider-1 to FortiManager output only. |
| **Output OS Version** | FortiOS 5.4 and 5.6 have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target. |
| **Discard unreferenced firewall objects** | Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.<br>This option can be useful if your target device has table size limitations.<br>You can view the unreferenced objects that FortiConverter removed on the Conversion Result page. |

| Setting | Description |
|---|---|
| **Ignore firewall policies with *all* or *any* addresses when processing NAT rules** | Specifies whether FortiConverter ignores firewall policies with an “all" or "any” address when it merges a NAT rule and a firewall policy to create a FortiGate NAT policy.<br><br>FortiConverter creates new policies in the output configuration based on where NAT rules to firewall policies intersect. Because firewall policies that use "all" or "any" as the address create many intersections, Fortinet recommends that you ignore them. |
| **Auto generate policy interfaces** | Specifies whether FortiConverter generates policy interfaces using a Check Point route file. (For example, a file you obtained using the `netstat -nr` command.)<br><br>You select the route file on the Firewall page.<br><br>Check Point policies define rules for network-to-network communication. When you migrate a Check Point configuration to FortiGate, which uses policies that define rules for interface-to-interface communication, you can use the Check Point router information to determine which interface a policy uses. If you disable this option, or no router information is not available, FortiConverter uses the "any" interface. |
| **More** | Displays additional start options. See Start Options - More on page 26. |
| **Output Directory** | Select the folder where the output configuration is saved. |

### Start Options - More

| Setting | Description |
|---|---|
| **Discard unreferenced firewall objects** | Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.<br><br>This option can be useful if your target device has table size limitations.<br><br>You can view the unreferenced objects that FortiConverter removed on the Conversion Result page. |
| **Auto generate policy interfaces** | Specifies whether FortiConverter generates policy interfaces using the Check Point route file.<br><br>Check Point policies define rules for network-to-network communication. When you migrate a Check Point configuration to FortiGate, which uses policies that define rules for interface-to-interface communication, you can use the Check Point router information to determine which interface a policy uses. If you disable this option, or no router information is not available, FortiConverter uses the "any" interface. |

| Setting | Description |
|---|---|
| **Adjust table sizes** | You can customize the maximum table sizes that FortiConverter uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 139. |
| **Number of year-long schedules from *day in month* schedules** | Specifies how many years of one-time schedules to generate.<br><br>The wizard converts Check Point “day in month” schedules into equivalent one-time FortiGate schedules. |
| **Enable Route-based IPSec** | Specifies whether Route-based IPSec is used for this conversion. |
| **Comments** | |
| **Interface comment** | Specifies whether FortiConverter copies the interface comment from the source configuration to the mapped FortiGate interface. |
| **Address comment** | Specifies whether FortiConverter copies the address comment from source configuration to the converted FortiGate address. |
| **Service comment** | Specifies whether FortiConverter copies the service comment from the source configuration to converted FortiGate service. |
| **Policy package name, rule Number**<br><br>**Original Check Point firewall rule comment**<br><br>**Policy package name, rule number, original Check Point firewall rule comment** | Specifies what information FortiConverter includes in the converted policy comment. |
| **NAT Merge** | |
| **Ignore firewall policies with *all* or *any* addresses when processing NAT rules** | Specifies whether FortiConverter ignores firewall policies with an “all" or "any” address when it merges a NAT rule and a firewall policy to create a FortiGate NAT policy.<br><br>FortiConverter creates new policies in the output configuration based on where NAT rules to firewall policies intersect. Because firewall policies that use "all" or "any" as the address create many intersections, Fortinet recommends that you ignore them. |
| **Enable Central NAT merge** | Specifies whether FortiConverter converts NATs to FortiGate central NATs instead of policy-based NATs. |

| Setting | Description |
|---|---|
| **Copy NAT merge policies to a separate text file** | Specifies whether FortiConverter generates a separate text file that lists the NAT rule intersections and the firewall policies they generated.<br><br>FortiConverter generates NAT merge policies by merging NAT and security rules in the source configuration. |
| **Enable *identity match* of NAT policy** | Specifies whether FortiConverter converts or ignores any identity NAT rules in the source configuration.<br><br>The "range" and "network" address objects in a Check point configuration can include hide NAT and static NAT. Check Point performs NAT only when a host in the IP range of the address object communicates with a host outside that range. To disable NAT for traffic with both source and destination inside the address range, Check Point generates an automatic rule called an "identity NAT rule".<br><br>By default, FortiConverter excludes this type of rule from the conversion because it performs no NAT after it is converted and generates redundant policies. You can enable this option to generate policies based on the identity NAT rules. |
| **Rule NAT merge depth**<br><br>**Static NAT merge depth**<br><br>**Hide NAT merge depth** | Specifies which types of NAT FortiConverter merges with the output firewall policies, or whether FortiConverter performs NAT merge based on object names or values.<br>• **Off** – FortiConverter converts firewall policies only and does not perform NAT merge for this type of NAT. This is useful for performing a quick, initial conversion to discover any conversion issues.<br>• **Object Names** – FortiConverter performs NAT merge based on matching address names in firewall policies and NAT rules.<br>• **Object Values** – FortiConverter performs NAT merge based on matching address values in firewall policies and NAT rules. It generates the most accurate matching of NAT rules and policies, but in most cases, it also generates more NAT policies.<br>Because it can take FortiConverter several hours to complete a conversion that include a large number of NAT rules, Fortinet recommends that you turn off or limit NAT merge for your initial conversion. Then, resolve any issues with the conversion before you run it again with NAT merge enabled.<br>For more information, including example matches, see NAT merge options on page 141. |
| **Back** | Displays the main Start Options page. |

### MDS Source Configuration (Provider-1 only)

| Setting | Description |
|---|---|
| **Browse** | Select the Provider-1 configuration files. |

### MDS Selection (Provider-1 only)

| Setting | Description |
|---|---|
| **Please select the MDS which you want to convert** | Select the domain to convert. |

### Global Policy Collection (Provider-1)

| Setting | Description |
|---|---|
| **Standard_Global_Policy** | Specifies whether FortiConverter converts the Standard Global Policy.<br><br>You can select both **Standard Global Policy** and **Simple Global Policy**. |
| **Simple_Global_Policy** | Specifies whether FortiConverter converts the Simple Global Policy. |

### Domain Source Configuration

A Check Point configuration is made up of management database files, which contain multiple object and policy definitions.

Ensure the configuration is in a text format (for example, in plain text or XML). FortiConverter cannot use binary files.

For more information, see Downloading the source configuration files on page 1.

| Setting | Description |
|---|---|
| **Browse** | Click to select domain source configuration files.<br><br>For information on acquiring these files, see Downloading the source configuration files on page 1. |

### Policy Collection

| Setting | Description |
|---|---|
| (policy collection item) | Select the policy collections to convert. |
| **Select/deselect all** | Select or clear all policy collection items. |

### Firewall Selection (SmartCenter only)

| Setting | Description |
|---|---|
| (firewall item) | Select one or more firewalls to convert from the domain source configuration.<br><br>If HA is configured, an entry for the HA device is displayed, in addition to the member gateways. |
| **Output to non-root VDOM** | Select to structure the conversion output for a VDOM-enabled device, using a VDOM you define.<br><br>By default, FortiConverter maps the firewall to a standalone FortiGate configuration that uses the FortiGate *root* VDOM. |
| (VDOM name field) | Enter the name of the VDOM to convert the firewall to. |
| (Route file name field) | If you selected **Auto generate policy interfaces** on the Start Options page, enter the path and file name of a file that contains route information, or click **Browse** to select it.<br><br>For example, the file can contain routing tables you obtained using the `netstat -nr` command. |

### Physical Interface Mapping (SmartCenter only)

To select the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.

To edit other values in the Interface Mapping dialog box, including changing the interface from physical to aggregate or unspecified, double-click a column other than FortiGate Interface.

The Interface Mapping dialog box allows you to select the following interface types:

- **aggregate** – Select up to four aggregate interface members. If you need to add additional members, edit the `set members interface` setting in the output configuration or use the FortiOS web UI to add interfaces after you import the configuration.
- **unspecified** – FortiConverter uses the interface name in the conversion, but ignores the type and other attributes, which provides a name-to-name mapping without interface configuration.

  For example, you can create resources such as VLANs, LAGs, and inter-VDOM links on the target FortiGate device before you import the conversion, and then reference those interfaces in the physical interface mapping.

You can also use the tuning page to create mappings, such as physical to VLAN, after the conversion is complete.

To delete an interface, select the entry and click **Delete**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

| Setting | Description |
|---|---|
| **FortiGate Interface** (table column) | Click to assign a FortiGate port for each interface.<br><br>Enter a port name or custom text. |
| **Import from file** | Click to load a set of interface mappings from a text file. |
| **Export current mappings** | Saves the current set of interface mappings to a text file. |
| **Add** | Click to add a mapping item. |
| **Edit** | Click to edit additional properties for the selected mapping item. |
| **Delete** | Click to delete the selected mapping item. |

## Route Information (SmartCenter only)

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

| Setting | Description |
|---|---|
| **Add** | Click to add a route. |
| **Edit** | Click to edit the selected route. |
| **Delete** | Click to delete the selected route. |

## Conversion Result

| Tab | Description |
|---|---|
| **Conversion Summary** | Provides statistics about the conversion. |
| **Policies Detected & Policies Created** | Allows you to view and compare the number of objects that FortiConverter detected in the source configuration and the ones it created for the output configuration. |
| **Messages & Warnings** | Allows you to review any objects that FortiConverter did not include in the conversion.<br><br>If you enabled **Discard unreferenced firewall objects** on the Start Page, this tab displays the objects that FortiConverter removed. |

| Setting | Description |
|---|---|
| **View in HTML** | Generates an HTML page of the conversion result. |
| **Go to Output** | Opens the output folder . |
| **Go to Tuning** | Opens the tuning page. See Tuning the FortiConverter output on page 108. |
| **Go to Report** | Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert. |

For more information, see Viewing the results of your automatic conversion on page 119

FortiConverter includes error and warning messages into the conversion when an error occurs.

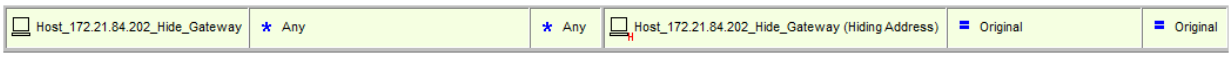
Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See "Error messages" on page 121 for more details.

# Check Point NAT merge examples

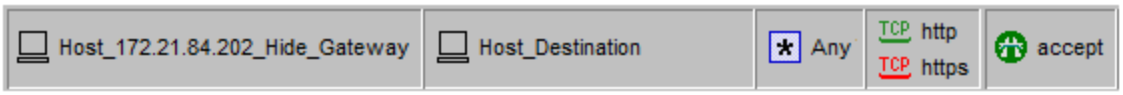
For more information about how FortiConverter handles NAT merges, see NAT merge options on page 141.

## Host address hides behind gateway

The source configuration hides the host address object `Host_172.21.84.202_Hide_Gateway` behind the gateway.




It also has a firewall rule that matches the object to source addresses.




FortiConverter generates the following policy, for which NAT is enabled (`set nat enable`). However, because it does not specify an IP pool, the source address uses the interface IP address to perform NAT:

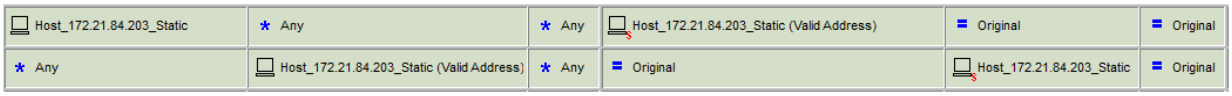
```
edit 10002
   set srcintf "port2"
   set dstintf "port1"
   set srcaddr "Host_172.21.84.202_Hide_Gateway"
   set dstaddr "Host_Destination"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
```

```
    set action accept
    set comments "Example of address hides behind gateway."
    set global-label "FW1"
    set nat enable
next
```

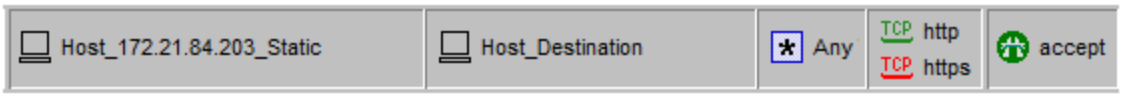
When a policy has NAT enabled, it attempts to match a source address to a VIP object. If it finds a match, it performs static NAT using the VIP object. If it does not find a match, it uses the interface IP address. (See Address with static NAT matches policy source address for an example with a VIP object.)

## Address with static NAT matches policy source address

The source configuration static NAT settings translate the IP address of the host address object `Host_172.21.84.203_Static` to `210.61.82.160`.




It also has a firewall rule that matches the object to source addresses.




FortiConverter generates the following VIP object and policy:

```
edit "vip-Host_172.21.84.203_Static"
    set extip 210.61.82.160
    set mappedip 172.21.84.203
    set extintf port1
    set nat-source-vip enable
next


edit 10003
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "Host_172.21.84.203_Static"
    set dstaddr "Host_Destination"
    set service "http" "https"
    set schedule "always"
    set logtraffic all
    set status enable
    set action accept
    set comments "Example of address with static NAT in source address."
    set global-label "FW1"
    set nat enable
next
```

When a policy has NAT enabled, it attempts to match a source address to a VIP object. If it finds a match, it performs static NAT using the VIP object. If it does not find a match, it uses the interface IP address. (See Host address hides behind gateway for an example without a VIP object.)

## Address with static NAT matches policy destination address

Like the example where static NAT matches the policy destination address, the source configuration static NAT settings translate the IP address of the host address object `Host_172.21.84.203_Static` to `210.61.82.160`.


It also has a firewall rule that matches the object to destinations.


FortiConverter generates the following VIP object and policy. The policy replaces the destination address with the VIP object:

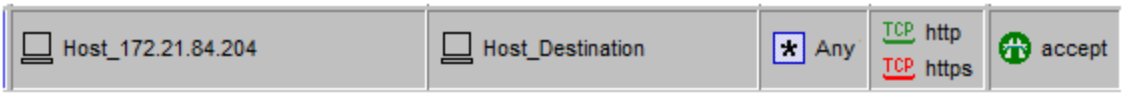
```
edit "vip-Host_172.21.84.203_Static"
   set extip 210.61.82.160
   set mappedip 172.21.84.203
   set extintf port1
   set nat-source-vip enable
next


edit 10004
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "Host_Source"
   set dstaddr "vip-Host_172.21.84.203_Static"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set comments "Example of address with static NAT in destination address."
   set global-label "FW1"
next
```

In this case, the destination address is used directly.

## Manual NAT rule matches policy source address with one-to-one mapping

A source configuration has a manual NAT rule that translates a source address:


It also has the following firewall rule:



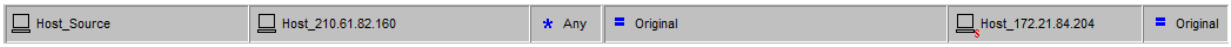

This configuration is a one-to-one mapping because both the original address and translated address are host addresses.

FortiConverter generates the following IP address pool and policy. NAT is enabled for the policy and it uses the pool to perform NAT:

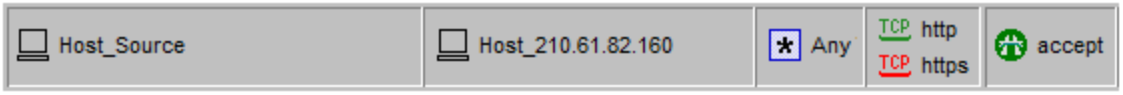
```
edit "ippool-210.61.82.160"
   set endip 210.61.82.160
   set startip 210.61.82.160
   set type overload
next


edit 10005
   set srcintf "port2"
   set dstintf "port1"
   set srcaddr "Host_172.21.84.204"
   set dstaddr "Host_Destination"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set comments "Example of one to one source NAT rule ."
   set global-label "FW1"
   set nat enable
   set poolname "ippool-210.61.82.160"
next
```

## Manual NAT rule matches policy destination address

A source configuration has a manual NAT rule that translates a destination address:




It also has the following firewall rule:




FortiConverter generates the following VIP object and policy:

```
edit "vip-Host_210.61.82.160"
   set extip 210.61.82.160
   set mappedip 172.21.84.204
   set extintf any
   set nat-source-vip enable
next


edit 10007
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "Host_Source"
   set dstaddr "Host_172.21.84.204"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
```

```
    set comments "Example of one to one destination NAT rule ."
    set global-label "FW1"
next
```

The translated address is used as the destination address because it is in internal network.

## NAT rule and policy addresses do not match: Destination address of the policy contains the NAT object

A source configuration has a host address object `Host_172.21.84.203_Static` that Static NAT translates to `210.61.82.160`.

| | | | | | |
|---|---|---|---|---|---|
| Host_172.21.84.203_Static | Any | Any | Host_172.21.84.203_Static (Valid Address) | Original | Original |
| Any | Host_172.21.84.203_Static (Valid Address) | Any | Original | Host_172.21.84.203_Static | Original |

It also has the following firewall rule:

| | | | | |
|---|---|---|---|---|
| Host_Source | AddressGroup_Destination | Any | TCP http<br>TCP https | accept |

`AddressGroup_Destination` is a group that contains the members `Host_172.21.84.203_Static`, `Host_Member3`, and `Host_Member4`.

FortiConverter generates the following VIP object and NAT policy:

```
edit "vip-Host_172.21.84.203_Static"
   set extip 210.61.82.160
   set mappedip 172.21.84.203
   set extintf port1
   set nat-source-vip enable
next


edit 00110009
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "Host_Source"
   set dstaddr "Host_172.21.84.203_Static"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set global-label "FW1"
next


edit 10009
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "Host_Source"
   set dstaddr "AddressGroup_Destination"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
```

```
    set status enable
    set action accept
    set comments "Example of name overlap in destination address."
    set global-label "FW1"
next
```

FortiConverter converts policy 10009 directly from the original firewall rule. Policy 0011009 is a copy of policy 10009 that has the destination address `Host_172.21.84.203_Static` and performs the static NAT.

### Unused VIP objects generate policy

In some cases, the final policy in an output configuration is one that FortiConverter generates from VIP objects that are not used as a destination address in at least one policy. For example:

```
edit 001
    set srcintf "port1"
    set dstintf "any"
    set srcaddr "all"
    set dstaddr "vip-Host_172.21.84.24" " vip-Host_172.21.84.25" " vip-Host_172.21.84.26"
        set service "ALL"
    set schedule "always"
    set logtraffic all
    set status enable
    set action deny
    set comments "This policy is auto-generated by FortiConverter to activate static-NAT
        VIPs that are not referenced in other policies."
next
```

This type of policy enables the source static NAT mapping by capturing all the VIP objects that other policies do not reference.

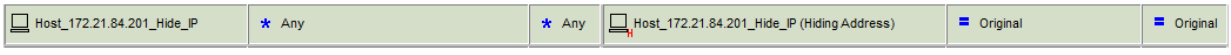
In some conversions, FortiConverter generates more than one of this kind of policy – one for each external interface that is referenced by an unreferenced VIP object.

## Check Point NAT merge examples with central NAT

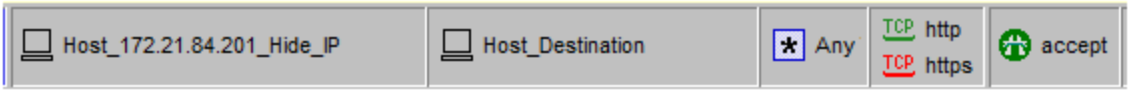
For more information about how FortiConverter handles NAT merges, see NAT merge options on page 141.

### Host address hides behind IP

The source configuration hides the host address object `Host_172.21.84.201_Hide_IP` behind the IP address `210.61.82.139`.




It also has a firewall rule that matches the object to source addresses.




FortiConverter captures the hide NAT IP address `210.61.82.139` in an IP pool:

```
edit "ippool-210.61.82.139"
    set endip 210.61.82.139
```

```
    set startip 210.61.82.139
    set type overload
next
```

FortiConverter also creates a central NAT object that uses the IP pool:

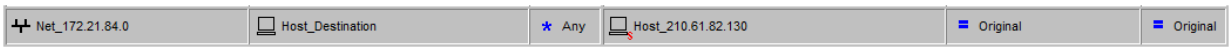
```
edit 3
    set orig-addr "Host_172.21.84.201_Hide_IP"
    set dst-addr "all"
    set nat-ippool "ippool-210.61.82.139"
next
```

FortiConverter converts the firewall policy to the following policy, for which central NAT is enabled ( `set nat enable` ):

```
edit 10001
    set srcintf "port2" (generated from route information)
    set dstintf "port1" (generated from route information)
    set srcaddr "Host_172.21.84.201_Hide_IP"
    set dstaddr "Host_Destination"
    set service "http" "https"
    set schedule "always"
    set logtraffic all
    set status enable
    set action accept
    set comments "Example of address hides behind IP."
    set global-label "FW1"
    set nat enable
next
```

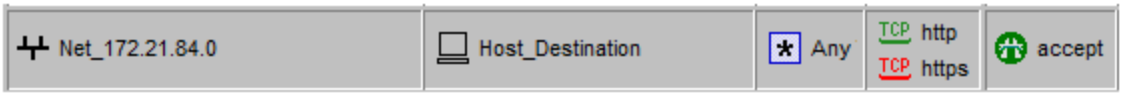
## Manual NAT rule matches policy source address with many-to-one mapping

A source configuration has a manual NAT rule that translates a source address:




`Net_172.21.84.0` is a network object with the IP address `172.21.84.0/24`.

The configuration also has the following firewall rule, which matches the object to source addresses:




FortiConverter converts many-to-one rules to an IP pool.

For this configuration, FortiConverter generates the following IP pool, central NAT object, and policy:

```
edit "ippool-210.61.82.130"
    set endip 210.61.82.130
    set startip 210.61.82.130
    set type overload
next
```

```
edit 2
    set orig-addr "Net_172.21.84.0"
    set dst-addr "Host_Destination"
```

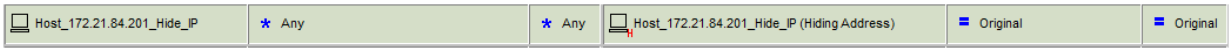
```
    set nat-ippool "ippool-210.61.82.130"
next


edit 10006
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "Net_172.21.84.0"
    set dstaddr "Host_Destination"
    set service "http" "https"
    set schedule "always"
    set logtraffic all
    set status enable
    set action accept
    set comments "Example of one to many source NAT."
    set global-label "FW1"
    set nat enable
next
```

## NAT rule and policy addresses do not match: Source address of the policy contains the NAT object

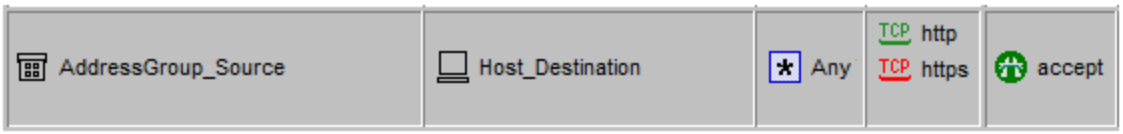
In some cases, the address field of a policy contains more than one address object. If NAT is enabled for an address object, FortiConverter calculates the overlap of the address object and the policy address. It then generates an independent policy ahead of the original policy.

FortiConverter uses this mechanism for all NAT types, including Hide NAT and Static NAT.

A source configuration has a host address object `Host_172.21.84.201_Hide_IP` that hides behind the address `210.61.82.139`.




It also has the following firewall rule:




`AddressGroup_Source` is a group that contains the members `Host_172.21.84.201_Hide_IP`, `Host_Member1`, and `Host_Member2`.

FortiConverter generates the following configuration, which converts the address `210.61.82.139` to an IP pool, and includes a central NAT object that uses the IP pool and a NAT-enabled policy:

```
edit "ippool-210.61.82.139"
    set endip 210.61.82.139
    set startip 210.61.82.139
    set type overload
next

edit 3
    set orig-addr "Host_172.21.84.201_Hide_IP"
    set dst-addr "all"
    set nat-ippool "ippool-210.61.82.139"
next
```

```
edit 00110008
   set srcintf "port2"
   set dstintf "port1"
   set srcaddr "Host_172.21.84.201_Hide_IP"
   set dstaddr "Host_Destination"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set global-label "MTKFW1"
   set nat enable
next

edit 10008
   set srcintf "port2"
   set dstintf "port1"
   set srcaddr "AddressGroup_Source"
   set dstaddr "Host_Destination"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set comments "Example of name overlap in source address."
   set global-label "FW1"
next
```

Policy 10008 is converted directly from the original firewall rule. Policy 0011008 is a copy of policy 10008 that specifies `Host_172.21.84.201_Hide_IP` as the source address and performs the hide NAT.

# Cisco conversions—legacy application

This section covers conversion from the Cisco IOS, IOS XR, and Nexus models. For conversion of the Cisco PIX, ASA, and FWSM models, see " Cisco conversions—new application" on page 48.

The conversions in this section uses the legacy FortiConverter application.

## Cisco differences

### General

- FortiGate's `set allowaccess` command for interfaces does not exist on Cisco firewalls. Because FortiGate requires this setting, FortiConverter enables all services for interfaces by default.
- The postfix "_conflict" used for services prevents a service and a service group from having the same name. It is recommended you rename these objects.
- On Cisco IPSec VPNs, Phase 1 (ISAKMP) supports more than two types of authentication methods. FortiGate supports only two types: `pre-share` and `rsa-sig`. Therefore, you must assign methods for each VPN connection. The wizard converts Cisco EZVPN configuration to FortiGate VPN policies with the srcintf "<tunnel-interface-name>" (i.e. phase1-interface object's name) and dstintf "any".
- For the conversion of Cisco devices managed by ADSM, address and service group settings are prepended with "DM_LINE_". The same names will be used in the conversion. Customers wanting to replace these names are recommended to do so after the conversion, using a text editor.
- FortiConverter does not support the following Cisco configuration elements:
  - Wild card netmasks for `access-list` and `object- group` objects
  - EZVPN conversion

    For example, FortiConverter does not support `crypto ipsec profile <profile-name>` and `crypto isakmp profile <profile-name>` .

### NAT support

| Software | Supported NAT types |
|---|---|
| **IOS** | Dynamic NAT and Static NAT |
| **PIX**<br>**FWSM**<br>**ASA (8.2 and earlier)** | Dynamic NAT(NAT exemption, policy dynamic NAT, regular)<br>Static NAT(Static NAT, Static PAT, Identity Static NAT) |
| **ASA (8.3 and later)** | Object NAT(Dynamic, Static)<br>Twice NAT |

FortiConverter does not support the following NAT features:

- ASA objects for NAT and double NAT
- Identity NAT and NAT Exemption

To reduce the number of NAT polices a conversion generates, FortiConverter does not convert Static NAT rules in which the source and mapped IPs are the same.

## Downloading the source configuration files

Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed. To acquire the configuration, enter the `show running-config` command, and then paste the output into a plain text file.

## Cisco conversion wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

### Start Options

| Setting | Description |
|---|---|
| **Model** | Select the model of the source configuration. |
| **Output Format** | Select the appropriate output format for your FortiGate device. |
| **Output OS Version** | FortiOS 5.4 and 5.6 have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target. |
| **Discard unreferenced firewall objects** | Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.<br><br>This option can be useful if your target device has table size limitations.<br><br>You can view the unreferenced objects that FortiConverter removed on the Conversion Result page. |
| **Copy NAT merge policies to a separate text file** | Specifies whether FortiConverter copies NAT merge policies to a separate text file named `PolicyMemo.txt` that lists the NAT rule intersections and the firewall policies they generated. |

| Setting | Description |
|---|---|
| **Adjust table sizes** | You can customize the maximum table sizes that FortiConverter uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 139. |
| **Include input configuration lines for each output policy** | Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment. |
| **Ignore firewall policies with *all* or *any* addresses when processing NAT rules** | Specifies whether FortiConverter ignores firewall policies with an “all" or "any” address when it merges a NAT rule and a firewall policy to create a FortiGate NAT policy.<br><br>FortiConverter creates new policies in the output configuration based on where NAT rules to firewall policies intersect. Because firewall policies that use "all" or "any" as the address create many intersections, Fortinet recommends that you ignore them. |
| **More** | Displays additional start options. See Start Options - More on page 43.<br><br>Available only when **Model** is **PIX**. |
| **Output Directory** | Select the folder where the output configuration is saved. |

## Start Options - More

| Setting | Description |
|---|---|
| **Enable Route-based IPSec** | Specifies whether Route-based IPSec is used for this conversion. |
| **NAT Merge** | |

| Setting | Description |
|---|---|
| **NAT exemption merge depth** | Specifies which types of NAT FortiConverter merges with the output firewall policies, or whether FortiConverter performs NAT merge based on object names or values.<br>• **Off** – FortiConverter converts firewall policies only and does not perform NAT merge for this type of NAT. This is useful for performing a quick, initial conversion to discover any conversion issues.<br>• **Object Names** – FortiConverter performs NAT merge based on matching address names in firewall policies and NAT rules.<br>• **Object Values** – FortiConverter performs NAT merge based on matching address values in firewall policies and NAT rules. It generates the most accurate matching of NAT rules and policies, but in most cases, it also generates more NAT policies.<br>Because it can take FortiConverter several hours to complete a conversion that include a large number of NAT rules, Fortinet recommends that you turn off or limit NAT merge for your initial conversion. Then, resolve any issues with the conversion before you run it again with NAT merge enabled.<br>For more information, including sample matches, see NAT merge options on page 141. |
| **Dynamic NAT merge depth** | |
| **Dynamic ACL NAT merge depth** | |
| **Static NAT merge depth** | |
| **Static ACL NAT merge depth** | |

## Source Configuration

| Setting | Description |
|---|---|
| **Source Configuration File** | Select the input file or files. |
| **Cisco Route File (Optional)** | Select a route file that FortiConverter uses to determine the interfaces used in output policies, in addition to routes it detects in the source configuration.<br>Because Cisco devices apply access-lists to source interfaces, FortiConverter can determine the source interfaces for output policies, but not the destination interfaces. When you specify a route file, FortiConverter uses the information in the file to determine the destination interface. Otherwise, it uses the "any" interface. |

## Context Selection

Map the virtual contexts in the source configuration to VDOMs in the output configuration.

By default, all virtual contexts are mapped to VDOMs with the same name. You can modify this default mapping as required by renaming VDOMs and removing virtual contexts from the conversion.

To select multiple items in the list, do one of the following:

- Select an item, and then Ctrl + click one or more additional items.
- Select an item, and then Shift + click an additional item. The items and any items between them are selected.

| Setting | Description |
|---|---|
| **Enable VDOM** | Select to enable VDOMs (add `config global` and `config vdom` syntax) to the output config. |
| **Add** | Click to add a mapping item after you have deleted one. |
| **Delete** | Click to delete a mapping item. |

## Physical Interface Mapping

To select the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.

To edit other values in the Interface Mapping dialog box, including changing the interface from physical to aggregate or unspecified, double-click a column other than FortiGate Interface.

The Interface Mapping dialog box allows you to select the following interface types:

- **aggregate** – Select up to four aggregate interface members. If you need to add additional members, edit the `set members interface` setting in the output configuration or use the FortiOS web UI to add interfaces after you import the configuration.
- **unspecified** – FortiConverter uses the interface name in the conversion, but ignores the type and other attributes, which provides a name-to-name mapping without interface configuration.

  For example, you can create resources such as VLANs, LAGs, and inter-VDOM links on the target FortiGate device before you import the conversion, and then reference those interfaces in the physical interface mapping.

You can also use the tuning page to create mappings, such as physical to VLAN, after the conversion is complete.

To delete an interface, select the entry and click **Delete**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

| Setting | Description |
|---|---|
| **FortiGate Interface** (table column) | Click to assign a FortiGate port for each interface.<br><br>Enter a port name or custom text. |
| **Import from file** | Click to load a set of interface mappings from a text file. |
| **Export current mappings** | Saves the current set of interface mappings to a text file. |
| **Add** | Click to add a mapping item. |
| **Edit** | Click to edit additional properties for the selected mapping item. |
| **Delete** | Click to delete the selected mapping item. |

## VLAN and Loopback

This page displays the logical interfaces that FortiConverter detects in the source configuration and the changes it makes to the associated physical interface and its naming.

You cannot use this page to modify the logical interface settings.

If required, you can use the Tuning page to modify logical interfaces and zones. See "Tuning the FortiConverter output" on page 108.

## Route Information

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

| Setting | Description |
|---|---|
| **Add** | Click to add a route. |
| **Edit** | Click to edit the selected route. |
| **Delete** | Click to delete the selected route. |

## VPN Phase2

| Setting | Description |
|---|---|
| **IKE Phase1** (table column) | Select an IKE Phase1 authentication method: **pre-share** (preshared keys) or **rsa-sig** (RSA signatures). |

## Conversion Result

| Tab | Description |
|---|---|
| **Conversion Summary** | Provides statistics about the conversion. |
| **Policies Detected & Policies Created** | Allows you to view and compare the number of objects that FortiConverter detected in the source configuration and the ones it created for the output configuration. |
| **Messages & Warnings** | Allows you to review any objects that FortiConverter did not include in the conversion.<br><br>If you enabled **Discard unreferenced firewall objects** on the Start Page, this tab displays the objects that FortiConverter removed. |

| Setting | Description |
|---|---|
| **View in HTML** | Generates an HTML page of the conversion result. |
| **Go to Output** | Opens the output folder . |
| **Go to Tuning** | Opens the tuning page. See Tuning the FortiConverter output on page 108. |
| **Go to Report** | Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert. |

For more information, see Viewing the results of your automatic conversion on page 119

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See "Error messages" on page 121 for more details.

# Cisco conversions—new application

This section covers conversion from the Cisco ASA, PIX, and FWSM models. For conversion of the Cisco IOS, IOS XR, and Nexus models, see "Cisco conversions—legacy application" on page 41.

The conversions in this section uses the new FortiConverter application.

For more information on new features available with the new application, see "New application features" on page 142.

## Cisco differences

### General

- FortiGate's `set allowaccess` command for interfaces does not exist on Cisco firewalls. Because FortiGate requires this setting, FortiConverter enables all services for interfaces by default.
- The postfix "_conflict" used for services prevents a service and a service group from having the same name. It is recommended you rename these objects.
- On Cisco IPSec VPNs, Phase 1 (ISAKMP) supports more than two types of authentication methods. FortiGate supports only two types: `pre-share` and `rsa-sig`. Therefore, you must assign methods for each VPN connection. The wizard converts Cisco EZVPN configuration to FortiGate VPN policies with the srcintf "<tunnel-interface-name>" (i.e. phase1-interface object's name) and dstintf "any".
- For the conversion of Cisco devices managed by ADSM, address and service group settings are prepended with "DM_LINE_". The same names will be used in the conversion. Customers wanting to replace these names are recommended to do so after the conversion, using a text editor.
- FortiConverter does not support the following Cisco configuration elements:
  - Wild card netmasks for `access-list` and `object- group` objects
  - EZVPN conversion

    For example, FortiConverter does not support `crypto ipsec profile <profile-name>` and `crypto isakmp profile <profile-name>` .

### NAT support

| Software | Supported NAT types |
|---|---|
| **IOS** | Dynamic NAT and Static NAT |
| **PIX**<br>**FWSM**<br>**ASA (8.2 and earlier)** | Dynamic NAT(NAT exemption, policy dynamic NAT, regular)<br>Static NAT(Static NAT, Static PAT, Identity Static NAT) |

| Software | Supported NAT types |
|---|---|
| **ASA (8.3 and later)** | Object NAT(Dynamic, Static)<br>Twice NAT |

FortiConverter does not support the following NAT features:

- ASA objects for NAT and double NAT
- Identity NAT and NAT Exemption

To reduce the number of NAT polices a conversion generates, FortiConverter does not convert Static NAT rules in which the source and mapped IPs are the same.

## Downloading the source configuration files

Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed. To acquire the configuration, enter the `show running-config` command, and then paste the output into a plain text file.

## Cisco conversion wizard

**To start a new conversion:**

1. Start the application and, using your web browser, connect to http://127.0.0.1:8000.
2. Click **New Conversion**, located at the top right corner.
   A popup dialog will appear.
3. Create and enter a name for the conversion configuration.
4. Select Cisco as the vendor.
5. Select a model to convert from.
6. Click **OK**.
7. Configure the conversion settings described in the following sections.

### Start

| Setting | Description |
|---|---|
| **Profile** | |
| **Description** | Enter a description of the configuration. |
| **Output Options** | |
| **Output Format** | Select the appropriate output format for your FortiGate device. |

| Setting | Description |
|---|---|
| **FOS Version** | FortiOS 5.4 and 5.6 have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target. |
| **Input** | |
| **Security Context Conversion** | Enable this option to convert configurations with multiple security contexts. |
| **Source Configuration** | Select the input file or files. This option only appears if Security Context Conversion is disabled. |
| **System Configuration** | Select the system configuration file. This file should include interfaces and config file names for each security context. This option only appears if Security Context Conversion is enabled. |
| **Context Configuration(.zip)** | Select the .zip file containing all the config files. The file name for each context should match the name given in the system configuration file. This option only appears if Security Context Conversion is enabled. |
| **Route File (Optional)** | Select a route file that FortiConverter uses to determine the interfaces used in output policies, in addition to routes it detects in the source configuration.<br><br>Because Cisco devices apply access-lists to source interfaces, FortiConverter can determine the source interfaces for output policies, but not the destination interfaces. When you specify a route file, FortiConverter uses the information in the file to determine the destination interface. |
| **Conversion Options** | |
| **Discard unreferenced firewall objects** | Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.<br><br>This option can be useful if your target device has table size limitations.<br><br>You can view the unreferenced objects that FortiConverter removed on the Conversion Result page. |
| **Adjust Service Table Capacity Size** | You can customize the maximum table sizes that FortiConverter uses when **Adjust Service Table Capacity Size** is selected. For more information, see Adjusting table sizes on page 139. |
| **Automatically generate policy interfaces** | Specifies whether FortiConverter automatically generates policy interfaces. |
| **Route-based IPSec** | Specifies whether Route-based IPSec is used for this conversion. |
| **Comment Options** | |

| Setting | Description |
|---|---|
| **Include input configuration lines for each output policy** | Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment. |
| **Address comment** | Specifies whether FortiConverter copies the address comment from the source configuration to the converted FortiGate address. |
| **Interface comment** | Specifies whether FortiConverter copies the interface comment from the source configuration to the converted FortiGate address. |
| **Service comment** | Specifies whether FortiConverter copies the service comment from the source configuration to the converted FortiGate address. |
| **NAT Merge Options** | |
| **Ignore firewall policies with *all* or *any* addresses when processing NAT rules** | Specifies whether FortiConverter ignores firewall policies with an “all" or "any” address when it merges a NAT rule and a firewall policy to create a FortiGate NAT policy.<br><br>FortiConverter creates new policies in the output configuration based on where NAT rules to firewall policies intersect. Because firewall policies that use "all" or "any" as the address create many intersections, Fortinet recommends that you ignore them. |
| **Enable central NAT merge** | Specifies whether FortiConverter converts NATs to FortiGate central NATs instead of policy-based NATs. |
| **Copy NAT merge policies to a separate text file** | Specifies whether FortiConverter copies NAT merge policies to a separate text file named `PolicyMemo.txt` that lists the NAT rule intersections and the firewall policies they generated. |
| **NAT Merge Depth** | |
| **Mode** | Specify the source version number. This option is available only when **Model** is **ASA**. |

| Setting | Description |
|---|---|
| **NAT exemption** | Specifies which types of NAT FortiConverter merges with the output firewall policies, or whether FortiConverter performs NAT merge based on object names or values. |
| **Dynamic NAT**<br>**Static NAT**<br>**Dynamic ACL NAT**<br>**Static ACL NAT** | • **Object Name Match** – FortiConverter performs NAT merge based on matching address names in firewall policies and NAT rules.<br>• **Object Content Overlap** – FortiConverter performs NAT merge based on matching address values in firewall policies and NAT rules. It generates the most accurate matching of NAT rules and policies, but in most cases, it also generates more NAT policies.<br>Because it can take FortiConverter several hours to complete a conversion that include a large number of NAT rules, Fortinet recommends that you turn off or limit NAT merge for your initial conversion. Then, resolve any issues with the conversion before you run it again with NAT merge enabled.<br>For more information, including sample matches, see NAT merge options on page 141. |

## Context Selection

Shows the source configuration before conversion.

By default, all virtual contexts are mapped to VDOMs with the same name.

Click on an option under Source Configuration Preview to display it. Use the search bars to filter the search.

## Interface Mapping

To select the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.

To edit other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns.

You can also use the tuning page to create mappings after the conversion is complete.

To import a set of interface mappings from a file, click **Import**. To download the current set of interface mappings, click **Export**.

To add an interface, click **New Interface**. A dialog box will allow you to configure the settings for the new interface.

To delete an interface, select the entry and click **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

| Setting | Description |
|---|---|
| **VDOM** | Shows the virtual domains used in the conversion. |

| Setting | Description |
|---|---|
| **Source Interface** | Shows each interface on the Cisco firewall. |
| **FortiGate Interface** | Shows the corresponding FortiGate interface. Click to assign a FortiGate port for each interface. |
| **Members** | Shows any members, if they are set. |
| **IP-Netmask** | Shows the IP address and netmask of the connection. |
| **Type** | Shows the type of interface. |
| **Access** | Shows which protocols has permission to access each interface. |
| **Import** | Click to load a set of interface mappings from a text file. |
| **Export** | Saves the current set of interface mappings to a text file. |
| **New Interface** | Click to add a new interface. |
| **Delete Selected** | Click to delete the selected mapping item. |

## Routing Information

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

| Setting | Description |
|---|---|
| **New Route** | Click to add a route. |
| **Delete Selected** | Click to delete the selected route. |

## Conversion Result

| Tab | Description |
|---|---|
| **Conversion Summary** | Provides statistics about the conversion. |
| **VDOM Mapping** | Shows how VDOMs were mapped from the source device to the new device. |
| **Interface Mapping** | Shows how interfaces were mapped for each VDOM from the source device. |

| Tab | Description |
|---|---|
| **Device Summary** | Provides statistics about the objects detected. |

For more details on how to fine-tune your conversion, see "New application tuning" on page 118.

To download your finished conversion, click **Download Configurations**, located in the top-right corner.Your conversion will be downloaded as a .zip file.

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See "Error messages" on page 121 for more details.

## Cisco PIX and ASA NAT merge examples

For more information about how FortiConverter handles NAT merges, see NAT merge options on page 141.

For ASA, these examples are valid only for source configurations created using software versions 8.2.x and earlier.

### Identity NAT

Dynamic NAT with ID 0 is the identity NAT and specifies that the address does not need to be translated. For example:

```
nat (inside) 0 172.17.3.68 255.255.255.255
```

Currently, because FortiConverter does not merge this kind of NAT, it ignores the settings when it converts the configuration.

### Static identity NAT

In the following settings, in the two static NAT settings, the real address and the mapped address are the same.

```
static (inside,outside) 200.251.129.33 200.251.129.33 netmask 255.255.255.255

static (inside,outside) 172.17.3.69 access-list inside_nat0_static

access-list inside_nat0_static extended permit ip host 172.17.3.69 object-
group Group0
```

FortiConverter does not support this kind of static NAT and it ignores the settings when it converts the configuration.

## Dynamic NAT with NAT IP

A source configuration has the following dynamic NAT settings:

```
global (outside) 1 172.31.242.69 netmask 255.255.255.255

nat (inside) 1 172.17.3.120 255.255.255.255
```

It also has the following firewall rule:

```
access-list acl_inside extended permit tcp host 172.17.3.120 object-group
Group_Destination eq http

access-group acl_inside in interface inside
```

FortiConverter generates the following IP pool and NAT policy from the source configuration:

```
edit "ippool-172.31.242.69"
   set endip 172.31.242.69
   set startip 172.31.242.69
   set type one-to-one
next


edit 10001
   set srcintf "port1" (corresponds to the interface “inside”)
   set dstintf "port2" (corresponds to the interface “outside”)
   set srcaddr "h_172.17.3.120"
   set dstaddr "Group_Destination"
   set service "HTTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
   set ippool enable
   set poolname "ippool-172.31.242.69"
next
```

The interface and address of the dynamic NAT matches the firewall rule, so FortiConverter inserts the IP pool into policy 10001.

## Dynamic NAT with mapped IP is “interface”

A source configuration has the following dynamic NAT settings:

```
global (outside) 2 interface

nat (inside) 2 172.17.40.73 255.255.255.255
```

It also has the following firewall rule:

```
access-list acl_inside extended permit tcp host 172.17.40.73 object-group
Group_Destination eq http

access-group acl_inside in interface inside
```

FortiConverter generates the following NAT policy from the source configuration:

```
edit 10002
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-172.17.40.73"
   set dstaddr "Group_Destination"
   set service "HTTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
next
```

The interface and address of the dynamic NAT matches the firewall rule. NAT is enabled for policy 10002, but because there is no IP pool specified, the source address uses the interface IP address to perform NAT.

## Dynamic policy NAT

A source configuration has the following dynamic NAT settings, which define NAT using an access list:

```
nat (inside) 1 access-list inside_nat_outbound
```

```
access-list inside_nat_outbound extended permit tcp host 172.17.40.70 host
200.185.36.43 eq http
```

```
global (outside) 1 172.31.242.69 netmask 255.255.255.255
```

It also has the following firewall rule, which matches the NAT settings:

```
access-list acl_inside extended permit tcp host 172.17.40.70 host
200.185.36.43 eq http
```

```
access-group acl_inside in interface inside
```

FortiConverter generates the following IP pool and NAT policy from the source configuration:

```
edit "ippool-172.31.242.69"
   set endip 172.31.242.69
   set startip 172.31.242.69
   set type one-to-one
next
```

```
edit 10003
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-172.17.40.70"
   set dstaddr "h-200.185.36.43"
   set service "HTTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
   set ippool enable
   set poolname "ippool-172.31.242.69"
next
```

The converted configuration is similar to when the source configuration specifies dynamic NAT with a NAT IP address.

FortiConverter converts the IP pool based on the dynamic NAT.

## Static NAT matches policy source address

A source configuration has the following static NAT settings:

```
static (inside,outside) 200.251.129.95 172.17.60.85 netmask 255.255.255.255
```

It also has the following firewall rule:

```
access-list acl_inside extended permit ip host 172.17.60.85 object-group
Group_Destination

access-group acl_inside in interface inside
```

FortiConverter converts the static NAT rule to a VIP object and generates a NAT policy:

```
edit "vip-200.251.129.95"
   set extip 200.251.129.95
   set mappedip 172.17.60.85
   set extintf port2
   set nat-source-vip enable
next


edit 10004
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-172.17.60.85"
   set dstaddr "Group_Destination"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
next
```

The NAT-enabled policy tries to match the source address to a VIP object. If it finds a match, it performs static NAT as the VIP object specifies. Otherwise, it uses the interface IP for NAT.

## Static NAT matches policy destination address

A source configuration has the following static NAT settings (which are the same as the example that matches by source address):

```
static (inside,outside) 200.251.129.95 172.17.60.85 netmask 255.255.255.255
```

It also has the following firewall rule:

```
access-list acl_outside extended permit ip any host 200.251.129.95

access-group acl_outside in interface outside
```

FortiConverter creates the same VIP object it does for the source address example, and the following NAT policy, which uses the VIP object as a destination address:

```
edit "vip-200.251.129.95"
   set extip 200.251.129.95
   set mappedip 172.17.60.85
   set extintf port2
   set nat-source-vip enable
next


edit 10005
   set srcintf "port2"
   set dstintf "port1"
   set srcaddr "all"
   set dstaddr "vip-200.251.129.95"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
next
```

## Static NAT that uses access list matches policy source address

A source configuration has the following settings, which define static NAT using an access list:

```
static (inside,outside) 172.31.242.69 access-list inside_nat_static
```

```
access-list inside_nat_static extended permit ip host 10.100.128.97 object-group Group_Destination
```

It also has the following firewall rule:

```
access-list acl_inside extended permit ip host 10.100.128.97 object-group Group_Destination
```

```
access-group acl_inside in interface inside
```

FortiConverter converts the static NAT settings to the following VIP object and policies:

```
edit "vip-172.31.242.69_ip"
   set extip 172.31.242.69
   set mappedip 10.100.128.97
   set extintf port2
   set nat-source-vip enable
next


edit 10006
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-10.100.128.97"
   set dstaddr "Group_Destination”
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
```

```
    set nat enable
next
```

The NAT-enabled policy tries to match the source address to a VIP object. If it finds a match, it performs static NAT as the VIP object specifies. Otherwise, it uses the interface IP for NAT.

## Static NAT specified by access list matches policy source address

The following source configuration settings define static NAT using an access list (they are the same as the example where static policy NAT matches the policy source address):

```
static (inside,outside) 172.31.242.69 access-list inside_nat_static
```

```
access-list inside_nat_static extended permit ip host 10.100.128.97 object-group Group_Destination
```

It also has the following firewall rule, which matches the NAT in source address:

```
access-list acl_outside extended permit ip object-group Group_Destination host 172.31.242.69
```

```
access-group acl_outside in interface outside
```

FortiConverter creates the same VIP object it does for the source address example, and the following NAT policy, which uses the VIP object as a destination address:

```
edit "vip-172.31.242.69_ip"
   set extip 172.31.242.69
   set mappedip 10.100.128.97
   set extintf port2
   set nat-source-vip enable
next


edit 100007
   set srcintf "por2"
   set dstintf "port1"
   set srcaddr "Group_Destination"
   set dstaddr "vip-172.31.242.69_ip"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
next


edit 10007
   set srcintf "port2"
   set dstintf "any"
   set srcaddr "Group_Destination"
   set dstaddr "h-172.31.242.69"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
next
```

## NAT rule and policy addresses do not match exactly

When a NAT rule address does not match a policy address exactly, FortiConverter calculates where the addresses intersect (overlap) and uses the result as the address for the NAT policy it generates.

### NAT rule address contains policy address

For example, a source configuration includes the following dynamic NAT configuration:

```
global (outside) 1 193.205.32.10 netmask 255.255.255.255
```

```
nat (inside) 1 10.1.2.0 255.255.255.0
```

It also contains the following firewall rule:

```
access-list acl_inside extended permit tcp host 10.1.2.1 host 193.205.23.66 eq
smtp
```

```
access-group acl_inside in interface inside
```

The NAT rule address `10.1.2.0 255.255.255.0` contains the firewall rule source address `10.1.2.1`.

FortiConverter converts the source NAT and firewall rules to the following IP pool and policies:

```
edit "ippool-193.205.32.0-193.205.32.255"
   set endip 193.205.32.10
   set startip 193.205.32.10
   set type one-to-one
next

edit 10001
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-10.1.2.1"
   set dstaddr "h-193.205.23.66"
   set service "SMTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
   set ippool enable
   set poolname "ippool-193.205.32.10"
next
```

The source address of rule 10001 is the intersection of the NAT rule and original rule, which is `"h-10.1.2.1"`.

### Policy address contains the NAT rule address

A source configuration includes the following NAT settings (which are the same as the example where the NAT rule address contains the policy address):

```
global (outside) 1 193.205.32.10 netmask 255.255.255.255
```

```
nat (inside) 1 10.1.2.0 255.255.255.0
```

It also contains the following firewall rule:

```
access-list acl_inside extended permit tcp 10.1.0.0 255.255.0.0 host
193.205.23.66 eq smtp

access-group acl_inside in interface inside
```

The firewall rule source address `10.1.0.0 255.255.0.0` contains the NAT rule address `10.1.2.0 255.255.255.0`.

FortiConverter converts the source NAT and firewall rules to the following IP pool and policies:

```
edit "ippool-193.205.32.0-193.205.32.255"
   set endip 193.205.32.10
   set startip 193.205.32.10
   set type one-to-one
next

edit 00110002
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "n-10.1.2.0_24"
   set dstaddr "h-193.205.23.66"
   set service "SMTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
   set ippool enable
   set poolname "ippool-193.205.32.10"
next


edit 10002
   set srcintf "port1"
   set dstintf "any"
   set srcaddr "n-10.1.2.0_16"
   set dstaddr "h-193.205.23.66"
   set service "SMTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
next
```

The policy 00110002 source address `"n-10.1.2.0_24"` is the intersection of NAT rule and firewall rule 10002.

## NAT rule matches address "all" in policy

A source configuration includes the following NAT settings (which are the same as the example where the NAT rule address contains the policy address):

```
global (outside) 1 193.205.32.10 netmask 255.255.255.255

nat (inside) 1 10.1.2.0 255.255.255.0
```

It also contains the following firewall rule:

```
access-list acl_inside extended permit tcp any host 193.205.23.66 eq smtp
```

```
access-group acl_inside in interface inside
```

The source address field is "any", which contains the NAT rule.

FortiConverter converts the source NAT and firewall rules to the following IP pool and policies:

```
edit 00110003
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "n-10.1.2.0_24"
   set dstaddr "h-193.205.23.66"
   set service "SMTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
   set ippool enable
   set poolname "ippool-193.205.32.10"
next


edit 10003
   set srcintf "port1"
   set dstintf "any"
   set srcaddr "all"
   set dstaddr "h-193.205.23.66"
   set service "SMTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
next
```

The policy 00110003 source address `"n-10.1.2.0_24"` is the intersection of NAT and firewall rules.

## Static NAT overlaps policy destination address

A source configuration has the following settings, which define static NAT using an access list:

```
static (inside,outside) 172.31.242.69 access-list inside_nat_static
```

```
access-list inside_nat_static extended permit ip host 10.100.128.97 object-
group Group_Destination
```

It also includes the following firewall rule:

```
access-list acl_outside extended permit ip object-group Group_Destination
172.31.242.0 255.255.255.0
```

```
access-group outside in interface outside
```

The firewall rule destination address `172.31.242.0 255.255.255.0` contains the static NAT mapped IP `172.31.242.69`.

FortiConverter generates the following VIP object and policies that use the object as a destination:

```
edit "vip-172.31.242.69_ip"
   set extip 172.31.242.69
   set mappedip 10.100.128.97
```

```
    set extintf port2
    set nat-source-vip enable
next


edit 100004
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "Group_Destination"
    set dstaddr "vip-172.31.242.69_ip"
    set service "ALL"
    set schedule "always"
    set logtraffic disable
    set status enable
    set action accept
next


edit 10004
    set srcintf "port2"
    set dstintf "any"
    set srcaddr "Group_Destination"
    set dstaddr "n-172.31.242.0_24"
    set service "ALL"
    set schedule "always"
    set logtraffic disable
    set status enable
    set action accept
next
```

### Static NAT overlaps address group object

A source configuration has the following settings, which define a static NAT using an access list:

```
static (inside,outside) 172.31.242.69 access-list inside_nat_static
```

```
access-list inside_nat_static extended permit ip host 10.100.128.97 object-group Group_Destination
```

The access list destination address `Group_Destination` contains two members:

```
object-group network Group_Destination
    network-object 10.255.253.0 255.255.255.0
    network-object 10.255.254.0 255.255.255.0
```

The source configuration also has a firewall rule that matches the static NAT rule and its destination is a member of the group `Group_Destination`.

```
access-list acl_inside extended permit ip host 10.100.128.97 10.255.253.0 255.255.255.0
```

```
access-group acl_inside in interface inside
```

FortiConverter generates the following NAT policy, which has the destination address `10.255.253.0 255.255.255.0`.

```
edit 10009
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "h-10.100.128.97"
```

```
    set dstaddr "n-10.255.253.0_24"
    set service "ALL"
    set schedule "always"
    set logtraffic disable
    set status enable
    set action accept
    set nat enable
next
```

## NAT exemption

NAT exemption is a dynamic policy NAT with ID 0. In most cases, you use NAT exemption to do one of the following:

- Exempt from NAT an address that is located in a NAT rule address range.
- In environments that use NAT control to block traffic to which no NAT rule applies, to permit this type of traffic.

### Exempt an address from a NAT rule

A source configuration has the following NAT exemption configuration:

```
nat (inside) 0 access-list inside_nat_exemption
```

```
access-list inside_nat_exemption extended permit ip host 172.13.100.88 object-group Group_Destination
```

It also has the following dynamic NAT rule:

```
nat (inside) 4 172.13.100.0 255.255.255.0
```

```
global (outside) 4 172.80.80.8 netmask 255.255.255.255
```

Both the NAT exemption and the dynamic NAT rule match the following firewall rule:

```
access-list acl_inside extended permit ip 172.13.100.0 255.255.255.0 object-group Group_Destination
```

```
access-group acl_inside in interface inside
```

FortiConverter generates the following policies:

```
edit 00110001
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "h-172.13.100.88"
    set dstaddr "Group_Destination"
    set service "ALL"
    set schedule "always"
    set logtraffic disable
    set status enable
    set action accept
next

edit 10001
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "n-172.13.100.0_24"
    set dstaddr "Group_Destination"
```

```
    set service "ALL"
    set schedule "always"
    set logtraffic disable
    set status enable
    set action accept
    set nat enable
    set ippool enable
    set poolname "ippool-172.80.80.8"
next
```

The NAT exemption configuration generates policy 00110001 with no NAT behavior. The dynamic NAT configuration generates policy 10001, which references an IP pool. Because 00110001 comes first in the configuration, it applies to address "h-172.13.100.88" before the policy used for address "n-172.13.100.0_24" (which applies dynamic NAT) is applied.

### Allowing traffic without NAT when PIX enables NAT control

When NAT control is enabled in PIX, traffic from an interface with high-level security to an interface with low-level security is not allowed if no NAT rule is configured. To allow traffic that does not require NAT, a NAT exemption is required.

The following NAT configuration is a source configuration, which includes NAT control and a NAT exemption:

```
nat-control

nat (inside) 0 access-list inside_nat_exemption

access-list inside_nat_exemption extended permit ip host 172.14.100.88 object-group Group_Destination
```

It also has the following firewall rule:

```
access-list acl_inside extended permit ip 172.14.100.0 255.255.255.0 object-group Group_Destination

access-group acl_inside in interface inside
```

The interface security level has the following configuration:

```
nameif ethernet0 outside security0

nameif ethernet1 inside security100
```

FortiConverter generates the following policies:

```
edit 00110002
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "h-172.14.100.88"
    set dstaddr "Group_Destination"
    set service "ALL"
    set schedule "always"
    set logtraffic disable
    set status enable
    set action accept
next

edit 10002
    set srcintf "port1"
    set dstintf "port2"
```

```
    set srcaddr "n-172.14.100.0_24"
    set dstaddr "Group_Destination"
    set service "ALL"
    set schedule "always"
    set logtraffic disable
    set status disable
    set action accept
    set comments "This policy is disabled as not allowed by NAT-Control."
next
```

The source interface of the firewall rule is "inside"(port1), which has security level 100. The destination interface of this firewall rule is calculated to be "outside"(port2), which has security level 0. Since "inside" has a higher security level than "outside", traffic from "n-172.14.100.0_24" to "Group_Destination" is not allowed if NAT is not configured (even if the firewall rule allows it). Only traffic from "h-172.14.100.88" to "Group_Destination" is allowed because a NAT exemption is configured for it. Since other traffic is not allowed, FortiConverter disables policy 10002, and adds a comment to show the reason.

## Unused VIP objects generate policy

In some cases, the final policy in an output configuration is one that FortiConverter generates from VIP objects that are not used as a destination address in at least one policy. For example:

```
edit 001
    set srcintf "port1"
    set dstintf "any"
    set srcaddr "all"
    set dstaddr "vip- 172.21.84.24" " vip- 172.21.84.25" " vip- 172.21.84.26"
    set service "ALL"
    set schedule "always"
    set logtraffic all
    set status enable
    set action deny
    set comments "This policy is auto-generated by FortiConverter to activate static-NAT
        VIPs that are not referenced in other policies."
next
```

This type of policy enables the source static NAT mapping by capturing all the VIP objects that other policies do not reference.

In some conversions, FortiConverter generates more than one of this kind of policy – one for each external interface that is referenced by an unreferenced VIP object.

# Palo Alto Networks conversion

## Palo Alto Networks OS (PAN-OS) differences

### Conversion support

FortiConverter does not support the following features

- VPN
- IPv6 address ranges
- IPv6 address subnets (will be supported in a future release)
- UTM

### NAT support

FortiConverter supports the conversion of Palo Alto Rule NAT only.

### Configuration notes

- PAN-OS handles NAT and firewall policies with two separate modules, while FortiGate handles NAT within its policy module. FortiConverter makes a best effort attempt to map NAT rules onto each policy during the conversion, but you should review the results for accuracy.
- FortiConverter converts PAN-OS weekly schedules to FortiGate weekday schedules that are stored in a schedule group.

## Downloading the source configuration files

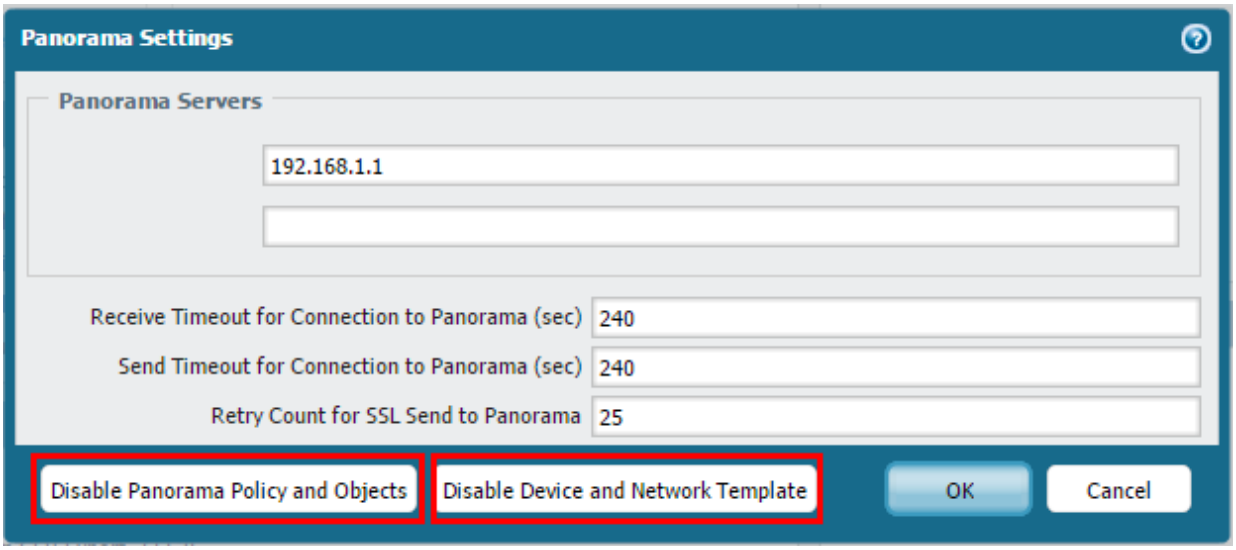
Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed.

In the web UI, go to **Device > Setup > Operations**, and then click **Export named configuration snapshot**.

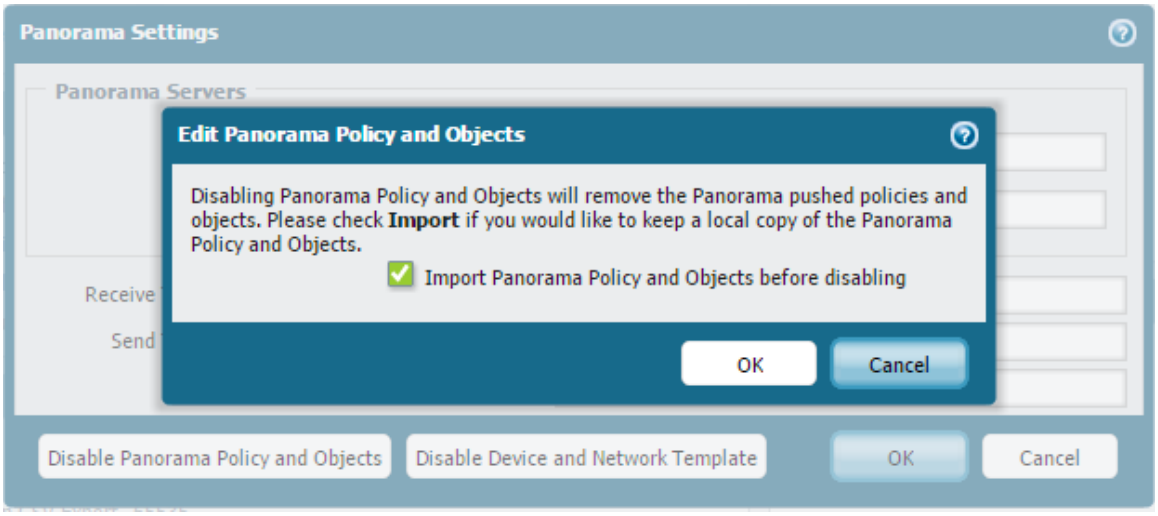
If the configuration is managed using Panorama shared policy configuration, you disable shared configuration before you export.

**To disable Panorama shared configuration**

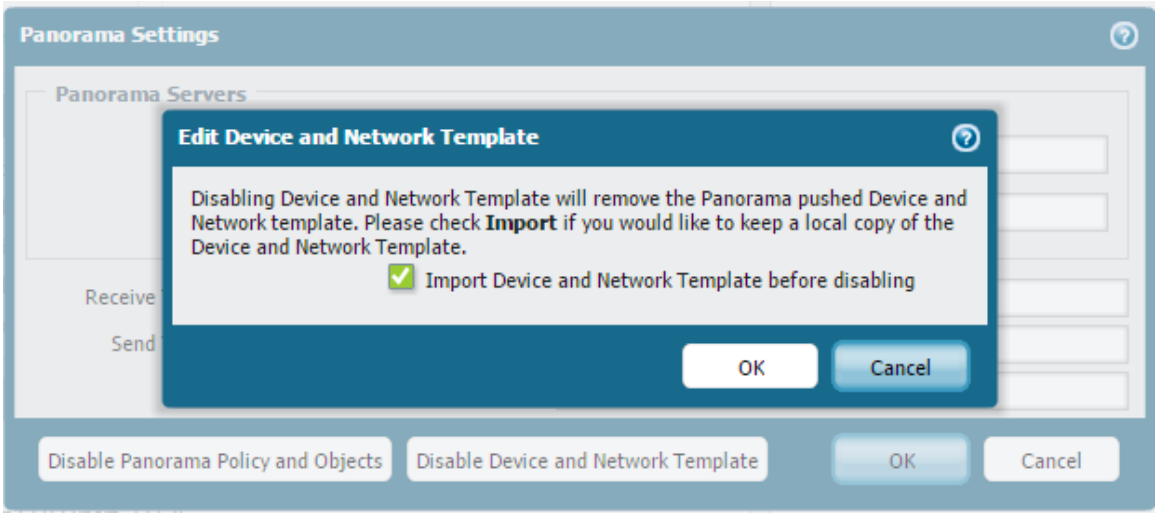
1. Log in to the device you want to remove from Panorama.
2. Go to **Device > Setup > Management > Panorama Settings** and click **Disable Panorama Policy and Object** or **Disable Device and Network Template**.



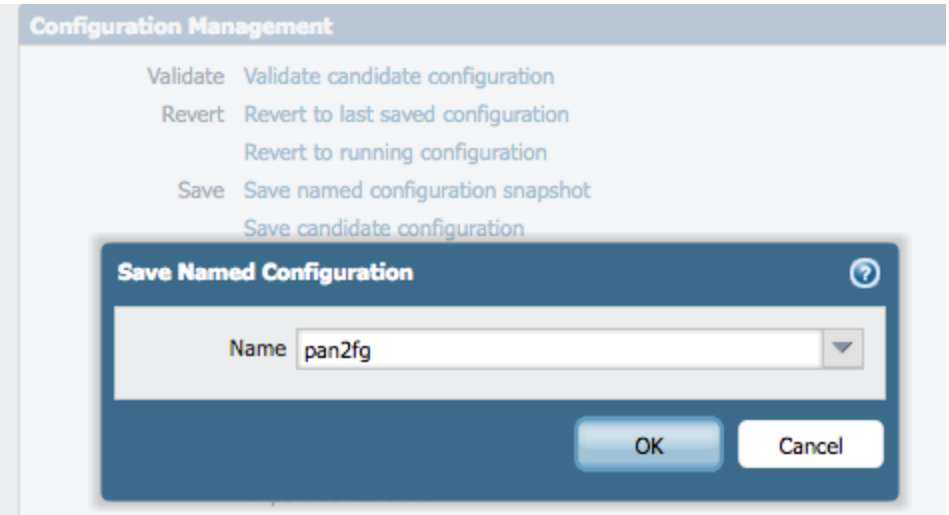

3. Do one of the following to import the configuration from Panorama into the firewall's local configuration:
   - If you clicked **Disable Panorama Policy and Object**, in the edit dialog box, select **Import Panorama Policy and Objects before disabling** and then click **OK**.



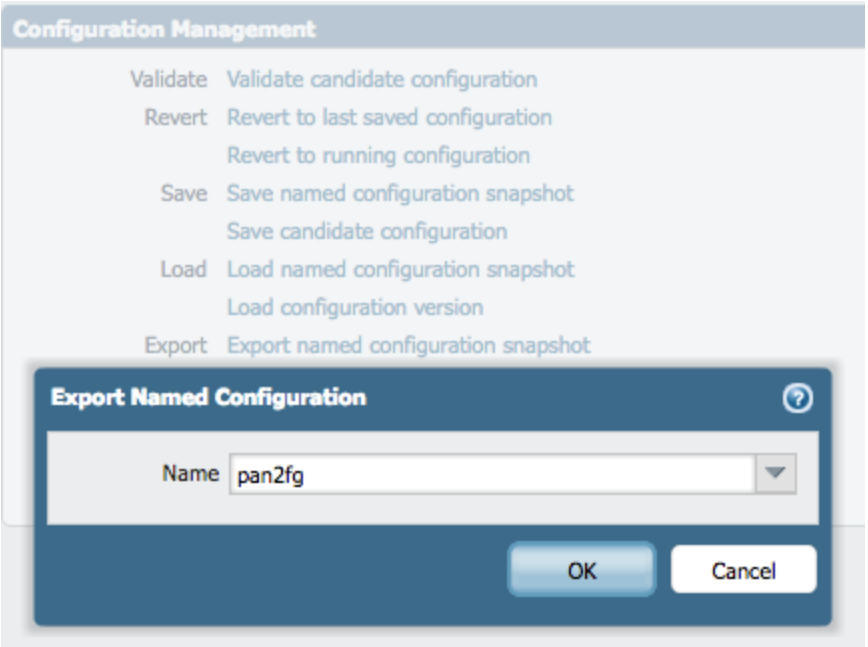

   - If you clicked **Disable Device and Network Template**, select **Import Device and Network Template before disabling** and then click **OK**.




4. Log in to the device that was removed from Panorama and go to **Device > Setup > Operations > Save > Save named configuration snapshot**.
5. Enter a name that helps to identify the configuration. In this example, it is **pan2fg**.



6. Go to **Device > Setup > Operations > Export > Export the named configuration snapshot**.




7. Click **OK**.

Select the exported file on the Source Configuration page of the Palo Alto conversion wizard.

## Palo Alto conversion wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

### Start Options

| Setting | Description |
|---|---|
| **Model** | Palo Alto is the only model supported. |
| **Output Format** | FortiGate is the only supported output. |
| **Output OS Version** | FortiOS 5.4 and 5.6 have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target. |

| Setting | Description |
|---|---|
| **Discard unreferenced firewall objects** | Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.<br><br>This option can be useful if your target device has table size limitations.<br><br>You can view the unreferenced objects that FortiConverter removed on the Conversion Result page. |
| **Ignore firewall policies *all* or *any* addresses** | Specifies whether FortiConverter ignores addresses with an “all” or "any" address when it merges a NAT rule and a security rule to create a FortiGate NAT policy. (In most cases, this type of address matches anything.) |
| **Include input configuration lines for each output policy** | Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment. |
| **Adjust table sizes** | You can customize the maximum table sizes that FortiConverter uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 139. |
| **Output Directory** | Select the folder where FortiConverter saves the output configuration. |

## Source Configuration

| Setting | Description |
|---|---|
| **Source Configuration File** | Select the input file or files. |

## VSYS Selection

Map the virtual systems in the source configuration to VDOMs in the output configuration.

To select multiple items in the list, do one of the following:

- Select an item, and then Ctrl + click one or more additional items.
- Select an item, and then Shift + click an additional item. The items and any items between them are selected.

| Setting | Description |
|---|---|
| **Enable VDOM** | Select to enable VDOMs (add `config global` and `config vdom` syntax) to the output config. |
| **Add** | Click to add a mapping item after you have deleted one. |
| **Delete** | Click to delete a mapping item. |

## Physical Interface Mapping

To select the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.

To edit other values in the Interface Mapping dialog box, including changing the interface from physical to aggregate or unspecified, double-click a column other than FortiGate Interface.

The Interface Mapping dialog box allows you to select the following interface types:

- **aggregate** – Select up to four aggregate interface members. If you need to add additional members, edit the `set members interface` setting in the output configuration or use the FortiOS web UI to add interfaces after you import the configuration.
- **unspecified** – FortiConverter uses the interface name in the conversion, but ignores the type and other attributes, which provides a name-to-name mapping without interface configuration.

  For example, you can create resources such as VLANs, LAGs, and inter-VDOM links on the target FortiGate device before you import the conversion, and then reference those interfaces in the physical interface mapping.

You can also use the tuning page to create mappings, such as physical to VLAN, after the conversion is complete.

To delete an interface, select the entry and click **Delete**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

| Setting | Description |
|---|---|
| **FortiGate Interface** (table column) | Click to assign a FortiGate port for each interface.<br>Enter a port name or custom text. |
| **Import from file** | Click to load a set of interface mappings from a text file. |
| **Export current mappings** | Saves the current set of interface mappings to a text file. |
| **Add** | Click to add a mapping item. |
| **Edit** | Click to edit additional properties for the selected mapping item. |
| **Delete** | Click to delete the selected mapping item. |

## Route Information

| Setting | Description |
|---|---|
| **Add** | Click to add a route. |
| **Edit** | Click to edit the selected route. |
| **Delete** | Click to delete the selected route. |

## Conversion Result

| Tab | Description |
|---|---|
| **Conversion Summary** | Provides statistics about the conversion. |
| **Policies Detected & Policies Created** | Allows you to view and compare the number of objects that FortiConverter detected in the source configuration and the ones it created for the output configuration. |
| **Messages & Warnings** | Allows you to review any objects that FortiConverter did not include in the conversion.<br><br>If you enabled **Discard unreferenced firewall objects** on the Start Page, this tab displays the objects that FortiConverter removed. |

| Setting | Description |
|---|---|
| **View in HTML** | Generates an HTML page of the conversion result. |
| **Go to Output** | Opens the output folder . |
| **Go to Tuning** | Opens the tuning page. See Tuning the FortiConverter output on page 108. |
| **Go to Report** | Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert. |

For more information, see Viewing the results of your automatic conversion on page 119

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See "Error messages" on page 121 for more details.

# Juniper conversions

## Juniper ScreenOS or Junos OS differences

### VLAN logical interfaces

FortiConverter recognizes interface names starting with "vlan" as logical interfaces.

### Service objects

Junos OS service objects support MS-RPS and SUN-RPC, where program-numbers (SUN) and UUID (MS) are used instead of ports. FortiOS supports this configuration using Application Control with an application override.

**Example of Junos service object conversion**

```
config application list
 edit "MS-ActiveDirectory"
  config entries
   edit 1
    set application 152305667
     config parameters
      edit 1
       set value "45f52c28-7f9f-101a-b52b-08002b2efabe"
      next
      edit 2
       set value "811109bf-a4e1-11d1-ab54-00a0c91e9b45"
      next
     end
    set action pass
   next
  end
 next
end

edit 10012
  set srcintf "trust"
  set dstintf "mgn"
  set srcaddr "MEI-Novi-172.24.81.0-24" "MEI-Novi-172.24.80.0-24" "MEI-Novi-
172.24.252.112-28"
  set dstaddr "MEI-WAN"
  set service "MS-ActiveDirectory"
  set schedule "always"
  set logtraffic all
  set status enable
  set action accept
  set comments "95"
```

```
  set application-list "MS-ActiveDirectory"
 next
```

### NAT support

For SRX Series gateways, FortiConverter supports the conversion of the following NAT types:

- Destination NAT
- Source NAT
- Static NAT

In ScreenOS, source NAT is implicitly enabled when: the destination zone is in the untrust-vr, the source zone is trust zone and the destination zone is untrust zone, and both belong to the trust-vr.

## Downloading the source configuration files

Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed.

For both ScreenOS and Junos, to obtain the configuration, in the web UI, go to **Configuration > Update > ConfigFile**.

Alternatively, for ScreenOS only, you can use the `get conf` CLI command and paste the output into a plain text file.

For Junos, FortiConverter requires the structural configuration file as a valid input. For example:

```
show configuration
## Last commit: 2013-06-05 11:28:53 CST by master
version 10.2S7;
groups {
    node0 {
        system {
            host-name SRX3400-Active;
            backup-router 172.16.1.254 destination 0.0.0.0/0;
        }
        interfaces {
            fxp0 {
                unit 0 {
                    family inet {
                        address 172.16.1.1/24;
                    }
                }
            }
        }
    }
.............
.............
```

# Juniper conversion wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

By default, output configurations from Juniper do not include some configuration information, including address and service comments. For an example of how to include this information in the output, see Including object comments in the output configuration on page 1.

## Start Options

| Setting | Description |
|---|---|
| **Model** | Select the model of the source configuration. |
| **Output Format** | Select the appropriate output format for your FortiGate device. |
| **Output OS Version** | FortiOS 5.4 and 5.6 have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target. |
| **Discard unreferenced firewall objects** | Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.<br><br>This option can be useful if your target device has table size limitations.<br><br>You can view the unreferenced objects that FortiConverter removed on the Conversion Result page. |
| **Include input configuration lines for each output policy** | Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment. |
| **Adjust table sizes** | You can customize the maximum table sizes that FortiMonitor uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 139. |
| **Output Directory** | Select the folder where the output configuration is saved. |

## Source Configuration Selection

| Setting | Description |
|---|---|
| **Source Configuration File** | Select the input file or files. |

## LSYS (Junos OS) or VSYS (ScreenOS) Selection

Map the logical or virtual systems in the source configuration to VDOMs in the output configuration.

To select multiple items in the list, do one of the following:

- Select an item, and then Ctrl + click one or more additional items.
- Select an item, and then Shift + click an additional item. The items and any items between them are selected.

| Setting | Description |
|---|---|
| **Enable VDOM** | Select to enable VDOMs (add `config global` and `config vdom` syntax) to the output config. |
| **Add** | Click to add a mapping item after you have deleted one. |
| **Delete** | Click to delete a mapping item. |

## Physical Interface Mapping

To select the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.

To edit other values in the Interface Mapping dialog box, including changing the interface from physical to aggregate or unspecified, double-click a column other than FortiGate Interface.

The Interface Mapping dialog box allows you to select the following interface types:

- **aggregate** – Select up to four aggregate interface members. If you need to add additional members, edit the `set members interface` setting in the output configuration or use the FortiOS web UI to add interfaces after you import the configuration.
- **unspecified** – FortiConverter uses the interface name in the conversion, but ignores the type and other attributes, which provides a name-to-name mapping without interface configuration.

  For example, you can create resources such as VLANs, LAGs, and inter-VDOM links on the target FortiGate device before you import the conversion, and then reference those interfaces in the physical interface mapping.

You can also use the tuning page to create mappings, such as physical to VLAN, after the conversion is complete.

To delete an interface, select the entry and click **Delete**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

| Setting | Description |
|---|---|
| **FortiGate Interface** (table column) | Click to assign a FortiGate interface for each interface.<br><br>Enter a port name or custom text. |
| **Import from file** | Click to load a set of interface mappings from a text file. |
| **Export current mappings** | Saves the current set of interface mappings to a text file. |

| Setting | Description |
|---|---|
| **Add** | Click to add a mapping item. |
| **Edit** | Click to edit additional properties for the selected mapping item. |
| **Delete** | Click to delete the selected mapping item. |

## Route Information

| Setting | Description |
|---|---|
| **Add** | Click to add a route. |
| **Edit** | Click to edit the selected route. |
| **Delete** | Click to delete the selected route. |

## Conversion Result

| Tab | Description |
|---|---|
| **Conversion Summary** | Provides statistics about the conversion. |
| **Policies Detected & Policies Created** | Allows you to view and compare the number of objects that FortiConverter detected in the source configuration and the ones it created for the output configuration. |
| **Messages & Warnings** | Allows you to review any objects that FortiConverter did not include in the conversion.<br><br>If you enabled **Discard unreferenced firewall objects** on the Start Page, this tab displays the objects that FortiConverter removed. |

| Setting | Description |
|---|---|
| **View in HTML** | Generates an HTML page of the conversion result. |
| **Go to Output** | Opens the output folder . |
| **Go to Tuning** | Opens the tuning page. See Tuning the FortiConverter output on page 108. |
| **Go to Report** | Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert. |

For more information, see Viewing the results of your automatic conversion on page 119

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See "Error messages" on page 121 for more details.

# SonicWall conversion

## SonicWall differences

### Special characters

FortiGate reserves '#' (hash sign), '(', and ')' (open and close curved brackets) as special characters. You cannot use them in the configuration unless an escape sequence precedes them. FortiConverter replaces these characters with the characters: '*' (star), '[' and ']' (open and close square brackets).

Examples:

- The address book "SNWL #1" becomes "SNWL *1".
- The service book "Citrix TCP (Session Reliability)" becomes "Citrix TCP [Session Reliability]".

### Address book configuration

- On FortiGate address objects do not support MAC addresses. Therefore, the wizard does not migrate SonicWall MAC addresses.
- FortiConverter generates two extra address book entries: "Any" and "_Address_Null".
  - "Any" is added because it is a default address book in SonicWall.
  - FortiConverter generates "_Address_Null" because FortiGate address groups do not allow a group without any members. Only empty address groups can refer to "_Address_Null".

### Service book configuration

- FortiConverter does not migrate SonicWall service objects that are predefined on FortiGate. For example, HTTP port 80 and HTTPS port 443.

### Schedule configuration

- A SonicWall schedule group can contain only one "one-time" schedule and multiple "recur" schedules. The "one-time" schedule is an implicit object that you can embed in the schedule group. Because FortiGate defines each schedule group explicitly, FortiConverter automatically generates "one-time" schedules for the SonicWall implicit schedules.
- FortiGate time schedule configuration does not support "24:00" (equal to the next day's 00:00). It uses "00:00" instead. When FortiConverter converts a SonicWall "recur" time schedule such as "M 00:00 to 24:00", it sets the end time to "00:00".

### Local User and User Group

- Because FortiConverter cannot parse the local user's password string, it sets all passwords to "123456".
- Unlike FortiConverter, SonicWall allows you to nest user groups. For example, in SonicWall, usergroup1 can be a member of usergroup1. FortiConverter removes any nested configurations.

### Route configuration

- FortiConverter does not convert the VPN configuration, including a Tunnel Interface VPN (route-based VPN).
- FortiConverter does not convert automatically generated routes like connected route and host route.

| Original source | Translated source | Original Destination | Translated Destination | Original Service | Translated Service |
|---|---|---|---|---|---|
| All Interface IP | X2 IP | Any | Original | Any | Original |

| Original source | Translated source | Original destination | Translated destination | Original service | Translated service |
|---|---|---|---|---|---|
| LAN Subnets | Original | WoW Static IP | X0 IP | SSLVPN | Original |

| Original source | Translated source | Original destination | Translated destination | Original service | Translated service |
|---|---|---|---|---|---|
| test_1112_grp | test_11_gw | test_12_gw | test_1211_grp | Echo | Original |

| Org Src | Tran Src | Org Dest | Tran Dest | Org Serv | Tran Serv |
|---|---|---|---|---|---|
| test_11_gw | test_12_gw | test_1112_grp | test_1211_grp | Echo | Original |

## Downloading the source configuration files

Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed. To download the configuration (*.exp file), in the web UI, go to **System > Settings > Export Settings**.

## SonicWall conversion wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

By default, output configurations from SonicWall do not include some configuration information, including address and service comments. For an example of how to include this information in the output, see Including object comments in the output configuration on page 1.

## Start Options

| Setting | Description |
|---|---|
| **Model** | SonicOS is the only model supported. |
| **Output Format** | Select the appropriate output format for your FortiGate device. |
| **Output OS Version** | FortiOS 5.4 and 5.6 have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target. |
| **Discard unreferenced firewall objects** | Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.<br><br>This option can be useful if your target device has table size limitations.<br><br>You can view the unreferenced objects that FortiConverter removed on the Conversion Result page. |
| **Ignore firewall policies with *all* or *any* addresses** | Specifies whether FortiConverter ignores firewall policies with an “all" or "any” address when it merges a NAT rule and a firewall policy to create a FortiGate NAT policy.<br><br>FortiConverter creates new policies in the output configuration based on where NAT rules to firewall policies intersect. Because firewall policies that use "all" or "any" as the address create many intersections, Fortinet recommends that you ignore them. |
| **Include input configuration lines for each output policy** | Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment. |
| **Adjust table sizes** | You can customize the maximum table sizes that FortiConverter uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 139. |
| **Output Directory** | Select the folder where FortiConverter saves the output configuration. |

## Source Configuration

| Setting | Description |
|---|---|
| **Source Configuration File** | Select the input file or files. |

## VSYS Selection

Map the virtual systems in the source configuration to VDOMs in the output configuration.

To select multiple items in the list, do one of the following:

- Select an item, and then Ctrl + click one or more additional items.
- Select an item, and then Shift + click an additional item. The items and any items between them are selected.

| Setting | Description |
|---|---|
| **Enable VDOM** | Select to enable VDOMs (add `config global` and `config vdom` syntax) to the output config. |
| **Add** | Click to add a mapping item after you have deleted one. |
| **Delete** | Click to delete a mapping item. |

## Physical Interface Mapping

To select the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.

To edit other values in the Interface Mapping dialog box, including changing the interface from physical to aggregate or unspecified, double-click a column other than FortiGate Interface.

The Interface Mapping dialog box allows you to select the following interface types:

- **aggregate** – Select up to four aggregate interface members. If you need to add additional members, edit the `set members interface` setting in the output configuration or use the FortiOS web UI to add interfaces after you import the configuration.
- **unspecified** – FortiConverter uses the interface name in the conversion, but ignores the type and other attributes, which provides a name-to-name mapping without interface configuration.

  For example, you can create resources such as VLANs, LAGs, and inter-VDOM links on the target FortiGate device before you import the conversion, and then reference those interfaces in the physical interface mapping.

You can also use the tuning page to create mappings, such as physical to VLAN, after the conversion is complete.

To delete an interface, select the entry and click **Delete**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

| Setting | Description |
|---|---|
| **FortiGate Interface** | Click to assign a FortiGate port for each interface. |
| (table column) | Enter a port name or custom text. |
| **Import from file** | Click to load a set of interface mappings from a text file. |
| **Export current mappings** | Saves the current set of interface mappings to a text file. |
| **Add** | Click to add a mapping item. |
| **Edit** | Click to edit additional properties for the selected mapping item. |
| **Delete** | Click to delete the selected mapping item. |

## VLAN and Loopback

This page displays the logical interfaces that FortiConverter detects in the source configuration and the changes it makes to the associated physical interface and its naming.

You cannot use this page to modify the logical interface settings.

If required, you can use the Tuning page to modify logical interfaces and zones. See "Tuning the FortiConverter output" on page 108.

## Route Information

| Setting | Description |
|---|---|
| **Add** | Click to add a route. |
| **Edit** | Click to edit the selected route. |
| **Delete** | Click to delete the selected route. |

## Conversion Result

| Tab | Description |
|---|---|
| **Conversion Summary** | Provides statistics about the conversion. |
| **Policies Detected & Policies Created** | Allows you to view and compare the number of objects that FortiConverter detected in the source configuration and the ones it created for the output configuration. |
| **Messages & Warnings** | Allows you to review any objects that FortiConverter did not include in the conversion.<br><br>If you enabled **Discard unreferenced firewall objects** on the Start Page, this tab displays the objects that FortiConverter removed. |

| Setting | Description |
|---|---|
| **View in HTML** | Generates an HTML page of the conversion result. |
| **Go to Output** | Opens the output folder . |
| **Go to Tuning** | Opens the tuning page. See Tuning the FortiConverter output on page 108. |
| **Go to Report** | Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert. |

For more information, see Viewing the results of your automatic conversion on page 119

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See "Error messages" on page 121 for more details.

# McAfee conversion

## StoneSoft differences

### VPNs

StoneSoft VPNs are not converted.

### Firewall clusters

Firewall clusters are not converted.

If a policy contains a firewall cluster, either remove or reconfigure the policy to remove the cluster. Other firewall cluster related configurations, such as routing nodes, are not converted.

## Downloading the source configuration files

If you encounter problems with your StoneSoft configuration file, send it to FortiConverter support at fconvert_feedback@fortinet.com. The FortiConverter team will help improve your conversion for you.

Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed.

The following is for McAfee Firewall Enterprise 7.0.1. The config is binary therefore the output of the following commands must be saved to a text file for FortiConverter.

- Interface and Zone (`cf interface|zone|zonegroup query`)
- Address object and address group object (`cf domain|ipaddr|iprange|subnet|netgroup query`)
- Service object and service group object (`cf service|servicegroup query`)
- Admin users and firewall users & user groups (`cf adminuser query`, `cf udb query`, `cf usergroup query`)
- Static routes (`cf static query`)
- Firewall Policy (`cf policy query`)

# McAfee conversion wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

## Start Options

| Setting | Description |
|---|---|
| **Model** | Select the model of the source configuration. |
| **Output Format** | FortiGate is the only supported output. |
| **Output OS Version** | FortiOS 5.4 and 5.6 have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target. |
| **Discard unreferenced firewall objects** | Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.<br>This option can be useful if your target device has table size limitations.<br>You can view the unreferenced objects that FortiConverter removed on the Conversion Result page. |
| **Include input configuration lines for each output policy** | Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment. |
| **Adjust table sizes** | You can customize the maximum table sizes that FortiMonitor uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 139. |
| **Output Directory** | Select the folder where FortiConverter saves the output configuration. |

## Source Configuration

| Setting | Description |
|---|---|
| **Source Configuration File** | Select the input file or files. |

## VSYS Selection

Map the virtual systems in the source configuration to VDOMs in the output configuration.

To select multiple items in the list, do one of the following:

- Select an item, and then Ctrl + click one or more additional items.
- Select an item, and then Shift + click an additional item. The items and any items between them are selected.

| Setting | Description |
|---|---|
| **Enable VDOM** | Select to enable VDOMs (add `config global` and `config vdom` syntax) to the output config. |
| **Add** | Click to add a mapping item after you have deleted one. |
| **Delete** | Click to delete a mapping item. |

## Physical Interface Mapping

To select the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.

To edit other values in the Interface Mapping dialog box, including changing the interface from physical to aggregate or unspecified, double-click a column other than FortiGate Interface.

The Interface Mapping dialog box allows you to select the following interface types:

- **aggregate** – Select up to four aggregate interface members. If you need to add additional members, edit the `set members interface` setting in the output configuration or use the FortiOS web UI to add interfaces after you import the configuration.
- **unspecified** – FortiConverter uses the interface name in the conversion, but ignores the type and other attributes, which provides a name-to-name mapping without interface configuration.

  For example, you can create resources such as VLANs, LAGs, and inter-VDOM links on the target FortiGate device before you import the conversion, and then reference those interfaces in the physical interface mapping.

You can also use the tuning page to create mappings, such as physical to VLAN, after the conversion is complete.

To delete an interface, select the entry and click **Delete**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

| Setting | Description |
|---|---|
| **FortiGate Interface** (table column) | Click to assign a FortiGate port for each interface.<br><br>Enter a port name or custom text. |
| **Import from file** | Click to load a set of interface mappings from a text file. |
| **Export current mappings** | Saves the current set of interface mappings to a text file. |
| **Add** | Click to add a mapping item. |
| **Edit** | Click to edit additional properties for the selected mapping item. |
| **Delete** | Click to delete the selected mapping item. |

## Route Information

| Setting | Description |
|---|---|
| **Add** | Click to add a route. |
| **Edit** | Click to edit the selected route. |
| **Delete** | Click to delete the selected route. |

## Conversion Result

| Tab | Description |
|---|---|
| **Conversion Summary** | Provides statistics about the conversion. |
| **Policies Detected & Policies Created** | Allows you to view and compare the number of objects that FortiConverter detected in the source configuration and the ones it created for the output configuration. |
| **Messages & Warnings** | Allows you to review any objects that FortiConverter did not include in the conversion.<br><br>If you enabled **Discard unreferenced firewall objects** on the Start Page, this tab displays the objects that FortiConverter removed. |

| Setting | Description |
|---|---|
| **View in HTML** | Generates an HTML page of the conversion result. |
| **Go to Output** | Opens the output folder . |
| **Go to Tuning** | Opens the tuning page. See Tuning the FortiConverter output on page 108. |
| **Go to Report** | Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert. |

For more information, see Viewing the results of your automatic conversion on page 119

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See "Error messages" on page 121 for more details.

# Tipping Point conversion

## Tipping Point differences

### Interface and schedule conversion

Source interfaces and destination interfaces are set to "any" after conversion.

Schedules are set to "always" in all policies after conversion.

### Action Set

If "Block" or "Drop" appears in an action set, the FortiGate policy strAction is set to "deny". Otherwise, the policy is set to "accept".

If "rsyslog" is found in an action set, the FortiGate policy strLogTraffic is set to "enable". Otherwise, it is disabled.

### Ignored fields

The following fields are parsed but ignored:

- Zone
- Users
- Apps
- Security
- Reputation
- Install On

## Downloading the source configuration files

If you encounter problems with your TippingPoint configuration file, send it to FortiConverter support at fconvert_feedback@fortinet.com. The FortiConverter team will help improve your conversion for you.

Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed.

To download your configuration files, copy them to a text file from TippingPoint SMS.

To download addresses and address groups:

1. Click the **Admin** tab, located at the top.
2. Click **Named resources**.
3. Click the address or address group.

4. Press Ctrl + A to select all.
5. Copy and paste the selected address or address group to a text file.
6. Repeat for all other addresses or address groups.

To download service and service groups:

1. Click the **Profile** tab, located at the top.
2. Click **Expand profiles**.
3. Click on **Shared settings**.
4. Click on the service or service group.
5. Press Ctrl + A to select all.
6. Copy and paste the selected service or service group to a text file.
7. Repeat for all other services and service groups.

To download policies:

1. Click the **Profile** tab, located at the top.
2. Click **Firewall profiles**.
3. Select a policy from the list.
4. Click on an item.
5. Press Ctrl + A to select all.
6. Copy and paste the policy to a text file.
7. Repeat for all other policies.

# Tipping Point conversion wizard

## Start Options

| Setting | Description |
|---|---|
| **Model** | IPS is the only model supported. |
| **Output Format** | FortiGate is the only supported output. |
| **Output OS Version** | FortiOS 5.4 and 5.6 have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target. |

| Setting | Description |
|---|---|
| **Discard unreferenced firewall objects** | Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.<br><br>This option can be useful if your target device has table size limitations.<br><br>You can view the unreferenced objects that FortiConverter removed on the Conversion Result page. |
| **Include input configuration lines for each output policy** | Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment. |
| **Adjust table sizes** | You can customize the maximum table sizes that FortiMonitor uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 139. |
| **Output Directory** | Select the folder where FortiConverter saves the output configuration. |

## Source Configuration

| Setting | Description |
|---|---|
| **Source Configuration File** | Select the input file or files. |

## VSYS Selection

Map the virtual systems in the source configuration to VDOMs in the output configuration.

To select multiple items in the list, do one of the following:

- Select an item, and then Ctrl + click one or more additional items.
- Select an item, and then Shift + click an additional item. The items and any items between them are selected.

| Setting | Description |
|---|---|
| **Enable VDOM** | Select to enable VDOMs (add `config global` and `config vdom` syntax) to the output config. |
| **Add** | Click to add a mapping item after you have deleted one. |
| **Delete** | Click to delete a mapping item. |

## Physical Interface Mapping

To select the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.

To edit other values in the Interface Mapping dialog box, including changing the interface from physical to aggregate or unspecified, double-click a column other than FortiGate Interface.

The Interface Mapping dialog box allows you to select the following interface types:

- **aggregate** – Select up to four aggregate interface members. If you need to add additional members, edit the `set members interface` setting in the output configuration or use the FortiOS web UI to add interfaces after you import the configuration.
- **unspecified** – FortiConverter uses the interface name in the conversion, but ignores the type and other attributes, which provides a name-to-name mapping without interface configuration.

  For example, you can create resources such as VLANs, LAGs, and inter-VDOM links on the target FortiGate device before you import the conversion, and then reference those interfaces in the physical interface mapping.

You can also use the tuning page to create mappings, such as physical to VLAN, after the conversion is complete.

To delete an interface, select the entry and click **Delete**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

| Setting | Description |
|---|---|
| **FortiGate Interface** (table column) | Click to assign a FortiGate port for each interface.<br><br>Enter a port name or custom text. |
| **Import from file** | Click to load a set of interface mappings from a text file. |
| **Export current mappings** | Saves the current set of interface mappings to a text file. |
| **Add** | Click to add a mapping item. |
| **Edit** | Click to edit additional properties for the selected mapping item. |
| **Delete** | Click to delete the selected mapping item. |

## Route Information

| Setting | Description |
|---|---|
| **Add** | Click to add a route. |
| **Edit** | Click to edit the selected route. |
| **Delete** | Click to delete the selected route. |

## Conversion Result

| Tab | Description |
|---|---|
| **Conversion Summary** | Provides statistics about the conversion. |
| **Policies Detected & Policies Created** | Allows you to view and compare the number of objects that FortiConverter detected in the source configuration and the ones it created for the output configuration. |
| **Messages & Warnings** | Allows you to review any objects that FortiConverter did not include in the conversion.<br><br>If you enabled **Discard unreferenced firewall objects** on the Start Page, this tab displays the objects that FortiConverter removed. |

| Setting | Description |
|---|---|
| **View in HTML** | Generates an HTML page of the conversion result. |
| **Go to Output** | Opens the output folder . |
| **Go to Tuning** | Opens the tuning page. See Tuning the FortiConverter output on page 108. |
| **Go to Report** | Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert. |

For more information, see Viewing the results of your automatic conversion on page 119

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See "Error messages" on page 121 for more details.

# Alcatel-Lucent conversion

## Alcatel-Lucent differences

### Conversion support

FortiConverter supports the conversion of the following Alcatel-Lucent Brick features:

- Interfaces
- Host Groups
- Service Groups
- Zone Brick Rulesets

Fortinet plans to support the following Lucent features in a future FortiConverter release:

- NAT
- Schedule
- VPN
- Hosts Behind Zone

### Address and address group configuration

- Lucent host addresses are mapped to FortiGate addresses.
- Lucent host groups are mapped to FortiGate address groups.
- Virtual Brick Addresses (VBA) are not supported.

### Interface configuration

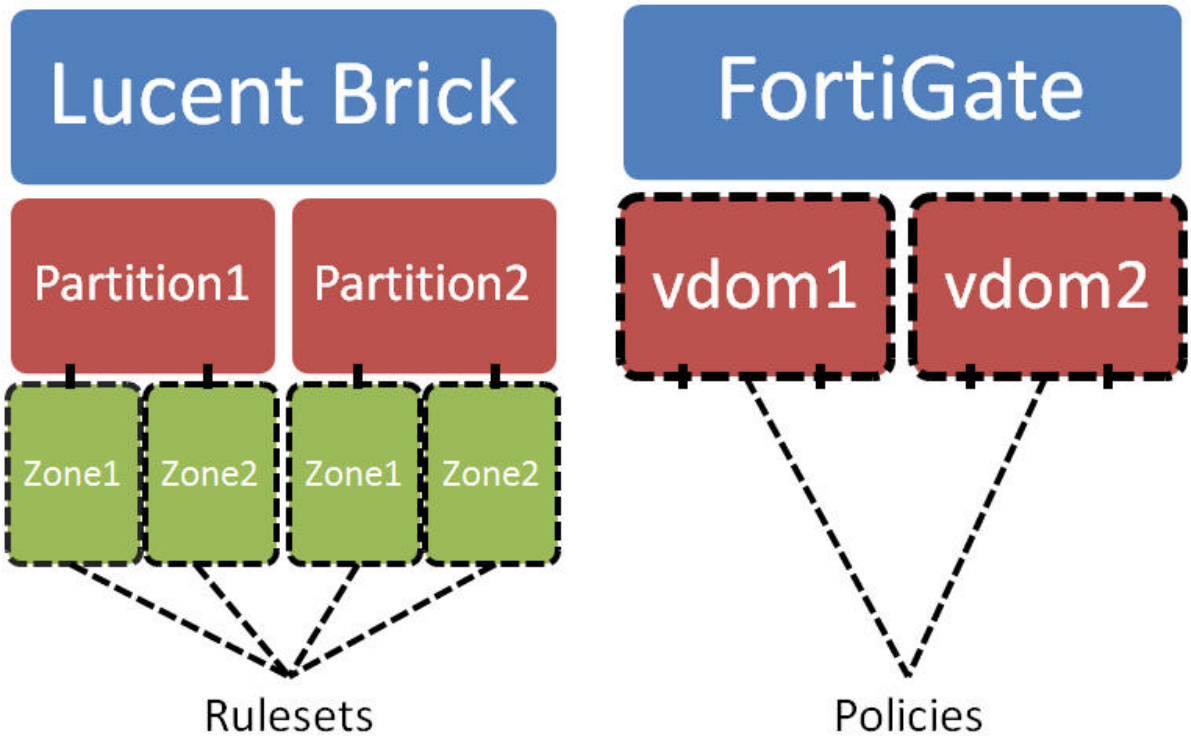
- FortiConverter assigns default VLAN configuration directly to physical interfaces.
- FortiConverter considers all VLANs named “*” or “Port Default” to be the default VLAN configuration.
- Domain Addresses are not supported.

### Service and Service Group configuration

- Lucent Service Groups are mapped to FortiGate Service Groups.
- Lucent service “*” maps to FortiGate service “any”.

### Policy configuration

Lucent Brick Zone Rulesets operate at the zone level, which has no direct equivalent in FortiGate. Zone rulesets need to be translated into equivalent FortiGate policies.




FortiConverter translates Lucent Brick rules by separating traffic into two categories: inter-partition and intra-partition.

- **Inter-partition traffic** behaves like inter-VDOM traffic, and is simple to convert to FortiGate policies.
- **Intra-partition traffic** is more complicated to convert because multiple zone rules can be applied.

FortiConverter handles the inter-partition traffic by creating a general policy for each rule.

FortiConverter handles the intra-partition traffic by looking for all matches between two zone rulesets. FortiConverter looks at 3 fields: source, destination, and service. All 3 fields must overlap for the rules to match. FortiConverter creates a policy for each match using the intersection of each field.

The action of the rules determines the action of the converted policy, as shown in the following table:

| Rule 1 | Rule 2 | Policy |
|---|---|---|
| Pass | Pass | Accept |
| Pass | Drop | Deny |
| Drop | Pass | Deny |
| Drop | Drop | Deny |

Inter-partition Deny policies have higher priority than intra-partition policies, while inter-partition Accept policies have lower priority than intra-partition policies.

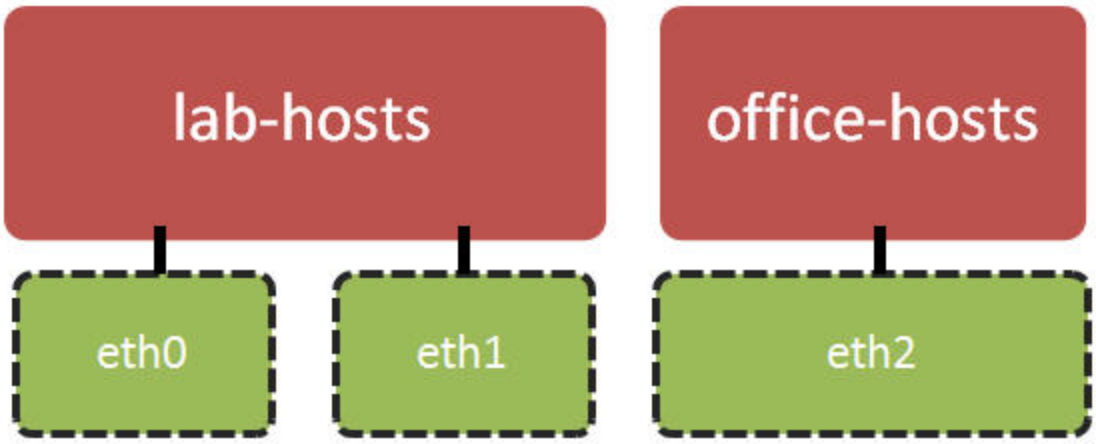
Lucent default ruleset “firewall” is currently unsupported.

## VDOM configuration

- Lucent partitions map to FortiGate VDOMs.
- VDOM names are limited to 11 characters. FortiConverter truncates longer names to 11 characters.
- Lucent partition “*Default” maps to the FortiGate root VDOM.

## Example conversion

The following block diagram and tables illustrates a Lucent configuration with 2 partitions and 3 zones.

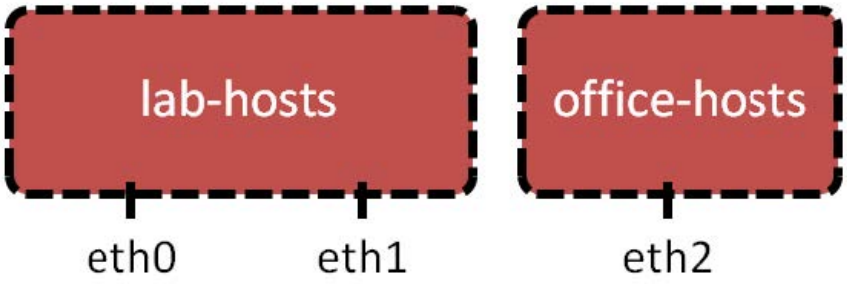



| Zone eth0 Ruleset | | | | | |
|---|---|---|---|---|---|
| **Rule Num** | **Direction** | **Source** | **Destination** | **Service** | **Action** |
| 1000 | Out | 192.168.1.15 | 172.30.10.1/24 | * | Drop |
| 1001 | Both | 192.168.1.0/24 | 172.30.10.1/24 | * | Pass |

| Zone eth1 Ruleset | | | | | |
|---|---|---|---|---|---|
| **Rule Num** | **Direction** | **Source** | **Destination** | **Service** | **Action** |
| 1000 | In | * | 172.30.10.5 - 172.30.10.20 | TCP | Pass |
| 1001 | Both | 192.168.1.132 | 172.30.10.9 | * | Pass |

| Zone eth2 Ruleset | | | | | |
|---|---|---|---|---|---|
| **Rule Num** | **Direction** | **Source** | **Destination** | **Service** | **Action** |
| 1000 | Both | * | 10.10.15.0/24 | HTTP | Pass |

This Lucent configuration creates the following FortiGate configuration. Inter-partition rules are in **bold**.




| VDOM lab-hosts Policies | | | | | | |
|---|---|---|---|---|---|---|
| **Policy Num** | **Src Interface** | **Dst Interface** | **Source** | **Destination** | **Service** | **Action** |
| **10000** | **eth0** | **any** | **192.168.1.15** | **172.30.10.1/24** | * | **Deny** |
| 10001 | eth0 | eth1 | 192.168.1.0/24 | 172.30.10.5 - 172.30.10.20 | TCP | Accept |
| 10002 | eth0 | eth1 | 192.168.1.132 | 172.30.10.9 | * | Accept |
| **10003** | **eth0** | **any** | **192.168.1.0/24** | **172.30.10.1/24** | * | **Accept** |
| 10004 | any | eth0 | 192.168.1.0/24 | 172.30.10.1/24 | * | Accept |
| 10005 | eth1 | eth0 | 192.168.1.132 | 172.30.10.9 | * | Accept |
| **10006** | **eth1** | **any** | **192.168.1.132** | **172.30.10.9** | * | **Accept** |
| **10007** | **any** | **eth1** | **192.168.1.132** | **172.30.10.9** | * | **Accept** |

| VDOM office-hosts Policies | | | | | | |
|---|---|---|---|---|---|---|
| **Policy Num** | **Src Interface** | **Dst Interface** | **Source** | **Destination** | **Service** | **Action** |
| **10000** | **any** | **eth2** | **any** | **10.10.15.0/24** | **HTTP** | **Accept** |
| **10001** | **eth2** | **any** | **10.10.15.0/24** | **any** | **TCP** | **Accept** |

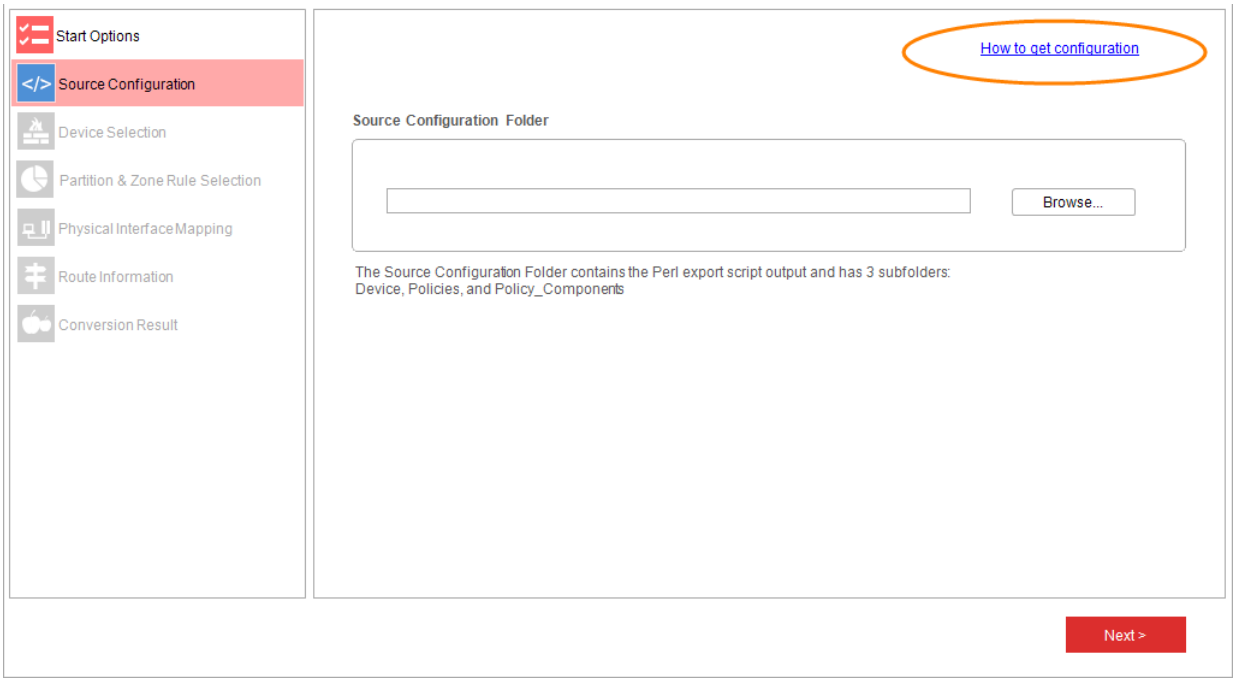
# Downloading the source configuration files

Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed. FortiConverter provides a Perl script for downloading Alcatel-Lucent Brick configurations.

### To access the Alcatel-Lucent configuration download script

1. On the FortiConverter home page, click the Alcatel-Lucent square.
2. On the Start Options page, click **Next**.

   If you are using the wizard to retrieve the download script only, use the default settings for this page. You can restart the wizard later after you have the file and are ready to perform the conversion with the appropriate settings.
3. On the Source Configuration Selection page, click **How to get configuration**.




The Windows folder that contains the Perl script and the documentation for using it are displayed. Follow the instructions to run the Perl script and output the source configuration as a set of directories.

# Alcatel-Lucent conversion wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

## Start Options

| Setting | Description |
|---|---|
| **Model** | LucentBrick is the only supported model. |
| **Output Format** | FortiGate is the only supported output format. |
| **Output OS Version** | FortiOS 5.4 and 5.6 have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target. |
| **Discard unreferenced firewall objects** | Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.<br><br>This option can be useful if your target device has table size limitations.<br><br>You can view the unreferenced objects that FortiConverter removed on the Conversion Result page. |
| **Enable *host behind zone* attribute** | Specifies whether FortiConverter restricts the destination or source IP addresses in the firewall policy it generates to ones specified by the "host behind zone" settings in the source configuration.<br><br>When this option is disabled, FortiConverter ignores the "host behind zone" settings and it uses the destination or source IP address specified by the source rule in the output policy. |
| **Convert *Administrative Zone* zone ruleset** | Specifies whether FortiConverter includes the default “administrativezone” ruleset in the output configuration.<br><br>Because the “administrativezone” ruleset is designed for device management, in most cases, it is not required in the output configuration. |
| **Include input configuration lines for each output policy** | Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment. |

| Setting | Description |
|---|---|
| **Enable *intra-partition* zone rule set merge** | Specifies whether FortiConverter creates FortiGate policies for traffic within a partition that the source configuration applies multiple zone rulesets to.<br><br>For more information on how FortiConverter converts intra-partition zone rulesets to a FortiGate policy, see Alcatel-Lucent conversion on page 96. |
| **Adjust table sizes** | You can customize the maximum table sizes that FortiConverter uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 139. |
| **Output Directory** | Select the folder where the output configuration is saved. |

## Source Configuration

| Setting | Description |
|---|---|
| **Source Configuration Folder** | Select the input folder. |

## Device Selection

| Setting | Description |
|---|---|
| (firewall name) | Select the firewalls to convert. |

## Partition & Zone Rule Selection

| Setting | Description |
|---|---|
| **Select all partitions** | Select to select all partitions and clear it to de-select all partitions. |
| **Partition selection** | Use the check box to select a partition to include in the conversion.<br><br>Click the pair of arrows on the right to open or close the detailed partition view, which shows the individual zone rules within a partition. |
| **Zone rule selection** | Use the check box to select a zone rule to include in the conversion. |

## Physical Interface Mapping

To select the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.

To edit other values in the Interface Mapping dialog box, including changing the interface from physical to aggregate or unspecified, either double-click a column other than FortiGate Interface, or select the entry and click **Edit**.

The Interface Mapping dialog box allows you to select the following interface types:

- **aggregate** – Select up to four aggregate interface members. If you need to add additional members, edit the `set members interface` setting in the output configuration or use the FortiOS web UI to add interfaces after you import the configuration.
- **unspecified** – FortiConverter uses the interface name in the conversion, but ignores the type and other attributes, which provides a name-to-name mapping without interface configuration.

  For example, you can create resources such as VLANs, LAGs, and inter-VDOM links on the target FortiGate device before you import the conversion, and then reference those interfaces in the physical interface mapping.

You can also use the tuning page to create mappings, such as physical to VLAN, after the conversion is complete.

To delete an interface, select the entry and click **Delete**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

| Setting | Description |
|---|---|
| **FortiGate Interface** (table column) | Click to assign a FortiGate port for each interface.<br><br>Enter a port name or custom text. |
| **Import from file** | Click to load a set of interface mappings from a text file. |
| **Export current mappings** | Saves the current set of interface mappings to a text file. |
| **Add** | Click to add a mapping item. |
| **Edit** | Click to edit additional properties for the selected mapping item. |
| **Delete** | Click to delete the selected mapping item. |

## VLAN and Loopback

This page displays the logical interfaces that FortiConverter detects in the source configuration and the changes it makes to the associated physical interface and its naming.

You cannot use this page to modify the logical interface settings.

If required, you can use the Tuning page to modify logical interfaces and zones. See "Tuning the FortiConverter output" on page 108.

## Route Information

| Setting | Description |
|---|---|
| **Add** | Click to add a route. |

| Setting | Description |
|---|---|
| **Edit** | Click to edit the selected route. |
| **Delete** | Click to delete the selected route. |

## Conversion Result

| Tab | Description |
|---|---|
| **Conversion Summary** | Provides statistics about the conversion. |
| **Policies Detected & Policies Created** | Allows you to view and compare the number of objects that FortiConverter detected in the source configuration and the ones it created for the output configuration. |
| **Messages & Warnings** | Allows you to review any objects that FortiConverter did not include in the conversion.<br><br>If you enabled **Discard unreferenced firewall objects** on the Start Page, this tab displays the objects that FortiConverter removed. |

| Setting | Description |
|---|---|
| **Export** | Generates an HTML page of the conversion result. |
| **Go to Output** | Opens the output folder . |
| **Go to Tuning** | Opens the tuning page. See Tuning the FortiConverter output on page 108. |
| **Go to Report** | Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert. |

For more information, see Viewing the results of your automatic conversion on page 119

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See "Error messages" on page 121 for more details.

# FortiGate configuration viewer

FortiConverter's new application provides a FortiGate configuration viewer. Use this configuration viewer to view interfaces, static routes, firewall policies and objects, NAT, and IPsec VPN on your FortiGate configurations.

The FortiGate configuration viewer is provided in place of the FortiGate conversion. The viewer helps FortiGate administrators manually migrate configurations from a FortiGate configuration file by providing a graphical interface to view polices and objects, and copy CLI.

Users who want to use the old FortiGate conversion for conversions up to FortiOS 5.4 can continue to use FortiConverter 5.3.0, which is available on the support site.

**To view a configuration:**

1. Start the application and, using your web browser, connect to http://127.0.0.1:8000.
2. Click **New Conversion**, located at the top-right corner.
   A dialog box will appear.
3. Create and enter a name for the configuration viewer.
4. Select Fortinet as the vendor.
5. Click **OK**.
   You will be brought to the Start page.
6. Click the  icon next to Source Configuration and select a FortiGate configuration file.
7. Click **Next**.
   If the configuration has no VDOMs, the wizard will skip Context Selection.

   You will be brought to the Conversion tuning page. Click on **FortiGate Configuration** to view the FortiOS configuration supported by the FortiConverter dataset. You cannot change your configuration from this page.

**To copy an object configuration:**

8. Navigate to the object type using the menu on the left.
   For example, to copy a Firewall policy configuration, go to the Firewall Policy section.
9. Click on the configurations you wish to copy.
10. Click **Copy CLI** , located on the bottom of the page.
    The selected configurations will be displayed.
11. Copy and paste the configurations to a text editor.
    From there, you can prepare your CLI commands to be run on the target device.

# Snort conversion

## Snort conversion wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

### Start Options

| Setting | Description |
|---|---|
| **Output FortiOS Version** | Select the version that corresponds to the FortiOS version on the target. |
| **Snort Rules** | Select the input file. |
| **No extra back slash "\"** | FortiConverter will not add an extra back slash to the conversion. |
| **Convert annotated rules as *status disable*** | Select to disable rules that are annotated in the source configuration. |
| **Adjust table sizes** | You can customize the maximum table sizes that FortiConverter uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 139. |
| **Snort Variable Definition** | Optionally, select the Snort variable definition file (for example, `snort.conf`) |
| **Output Directory** | Select the folder where FortiConverter saves the output configuration. |

### Rule Variables

| Setting | Description |
|---|---|
| **IP Variables** | Click a value to edit it, if required. |
| **Port Variables** | Click a value to edit it, if required. |

## Conversion Result

| Setting | Description |
|---|---|
| **Go to Output** | Opens the output folder . |
| **Go to Report** | Opens an HTML page that displays the conversion mapping. |

For more information, see Viewing the results of your automatic conversion on page 119

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See "Error messages" on page 121 for more details.

# Tuning the FortiConverter output

## Legacy application tuning

Although FortiConverter attempts to automatically convert as much of the source configuration as possible, in some cases, your input is required to complete the conversion. The Tuning page allows you to tune the results for your environment. To access the Tuning page, on the Conversion Result page, click **Go to Tuning**.

When you navigate to the Tuning page for the first time, FortiConverter prompts you to save the current output (the initial conversion). This backed-up conversion allows you to revert or refer to the initial conversion later, if needed.

If you are running the trial license, you can use the Tuning page to review your conversion, which is helpful if you are evaluating FortiConverter.

To quickly view a tuning "snapshot" (a configuration that you exported from the tuning page earlier), open the wizard for the appropriate vendor, click **Tuning** on any page, and then navigate to the snapshot file to import it.

You can add, modify, or delete firewall policies and objects, as well as interfaces and zones. FortiConverter applies any modifications you make immediately.

### Toolbar options

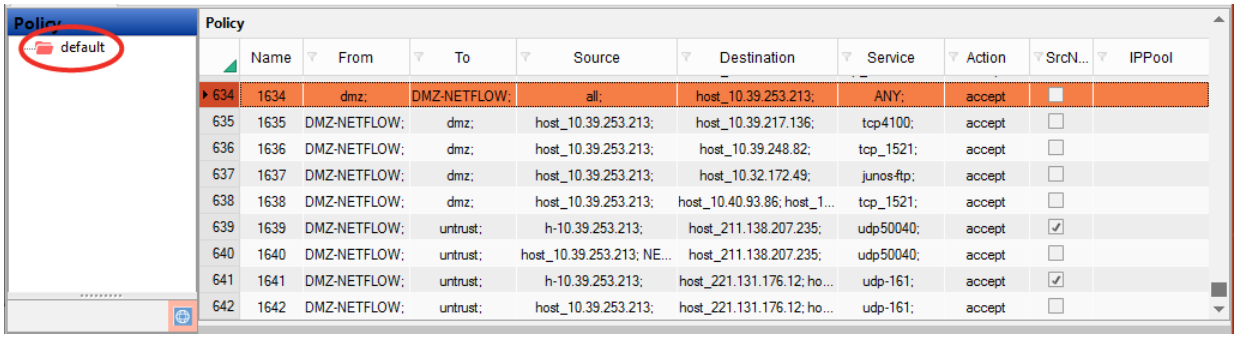
| Item | Description |
|---|---|
| **Home** | Click to return to the main page. |
| **Help** | Click to open the latest version of this guide. |
| **Back** | Click to return to the Conversion Result page. FortiConverter preserves any changes but does not save them in an output file. (Use **Go to Report** to save changes to an output file.) |
| **Backup** | Click to save the current configuration, including any modifications, to a text file (a tuning "snapshot"). |
| **Restore** | Click to import a configuration you exported earlier (a tuning "snapshot"). FortiConverter discards any changes in the current configuration. |

| Item | Description |
|---|---|
| **Export Policies** | Click to export policies as a comma-separated values (CSV) format file.<br><br>This can be helpful if you want to work in a spreadsheet application, share the conversion with a team of reviewers, or import bulk changes. |
| **Import Policies** | Click to import policies from a comma-separated values (CSV) format file. FortiConverter replaces the current policies with the ones in the CSV file and rebuilds the relationship between the policies and objects. |
| **VDOM** | Select the VDOM in the output to display in the Tuning page. |
| **Go to Report** | Click to view the configuration output in HTML format.<br><br>The report included converted and non-converted objects and a summary of the conversion. |
| **Go to Output** | Click to view the files for the current configuration, including any modifications. |

## Policy Tuning tab

The Policy Tuning tab allows you to review output policies and converted objects.

To review output policies, in the Policy navigation pane, select a package. The converted policies in the package are displayed.

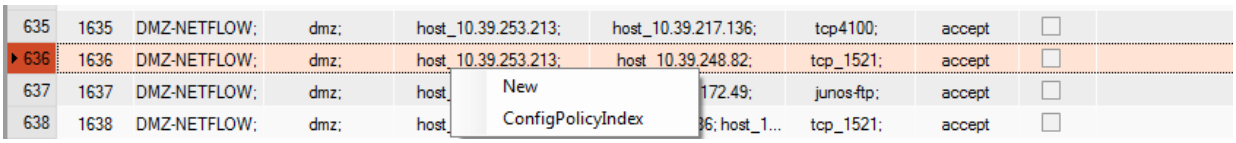



### To add a new policy to a package

1. Right-click a policy, and then click **New**.
2. Complete the settings, and then click **OK**.

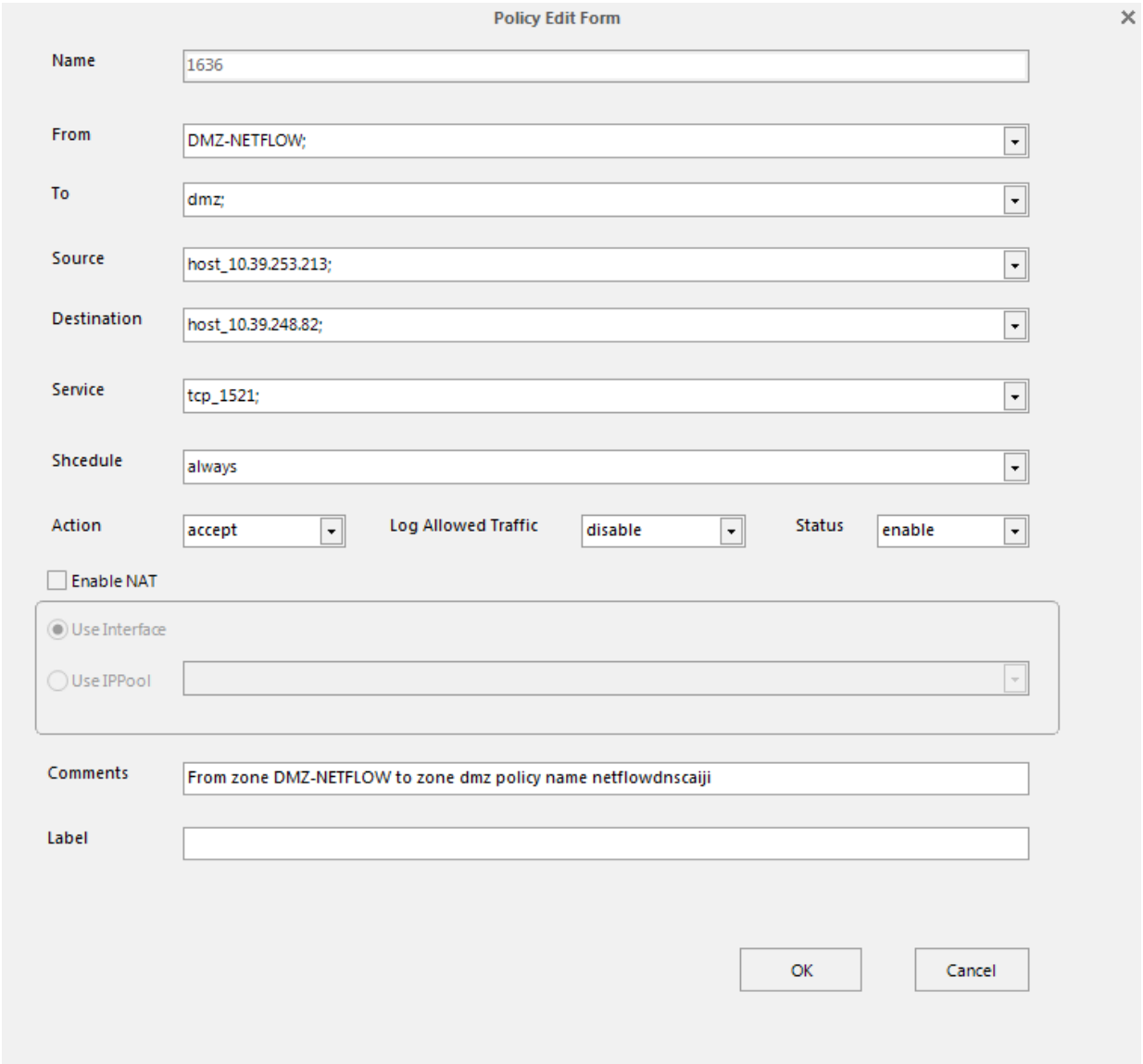
### To renumber the policies

1. Right-click the policy where you want the numbering to restart, and then click **ConfigPolicyIndex**.
2. For **Set Policy Index Start With**, enter the initial policy number to use, and then click **OK**.




### To edit the details for a converted policy

Double-click the policy and edit the settings as required.



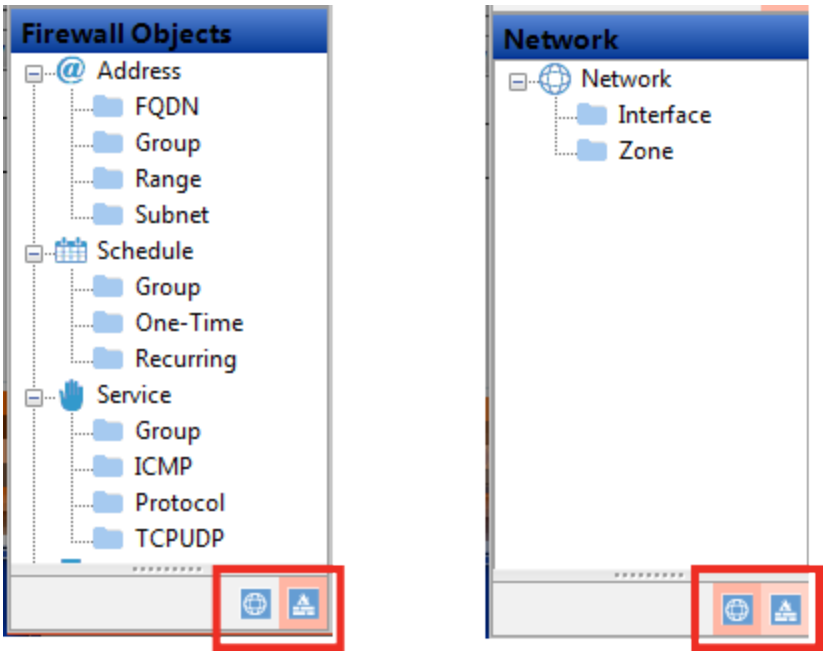

| Item | Description |
|---|---|
| **Name** | You cannot edit this value. |
| **From** | Select source interface(s). |

| Item | Description |
|---|---|
| **To** | Select destination interface(s). |
| **Source** | Select source address object(s). |
| **Destination** | Select destination address object(s). |
| **Service** | Select service object(s). |
| **Schedule** | Select schedule object. – select to enable NAT, and then select to use Interface or IPPool Comments – modify the comments for the policy Label – modify the label of the policy |
| **Action** | Specify whether traffic is accepted or denied. |
| **Log Allowed Traffic** | Specify whether logging is enabled. |
| **Status** | Specify whether the policy is enabled. |
| **Enable NAT** | Select to enable NAT, and then do one of the following:<br>• Select **User Interface**.<br>• Select **Use IPPool** and specify a pool. |
| **Comments** | Edit the comments for the policy. |
| **Label** | Edit the label for the policy. |

**To review and edit firewall objects and interfaces**

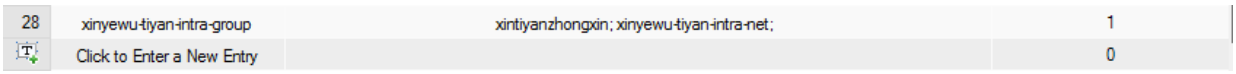
1. Go to the navigation pane at the bottom-left of the Policy Tuning tab.

   Click the icons at the bottom of the pane to switch between firewall objects and interfaces.




2. To view objects, select a category in the navigation pane.


3. To add a new object, scroll to the bottom of the list, click in an empty row, and then complete the fields as required.




4. The PolicyRef column displays the number of policies that reference that firewall object.

   Click the PolicyRef. column for the entry to display the specific policies in the Policy table above.

   You cannot delete objects that are referenced by any other part of the configuration.

### To filter rows to display only matching data

You can filter every column that has the [filter mark] by a given option or custom expression.

### To delete a line of the configuration

Click the policy or object you want to delete to select it, and then press the Delete key on your keyboard.

You cannot delete items that are used by another policy or group.

### To reorder rows

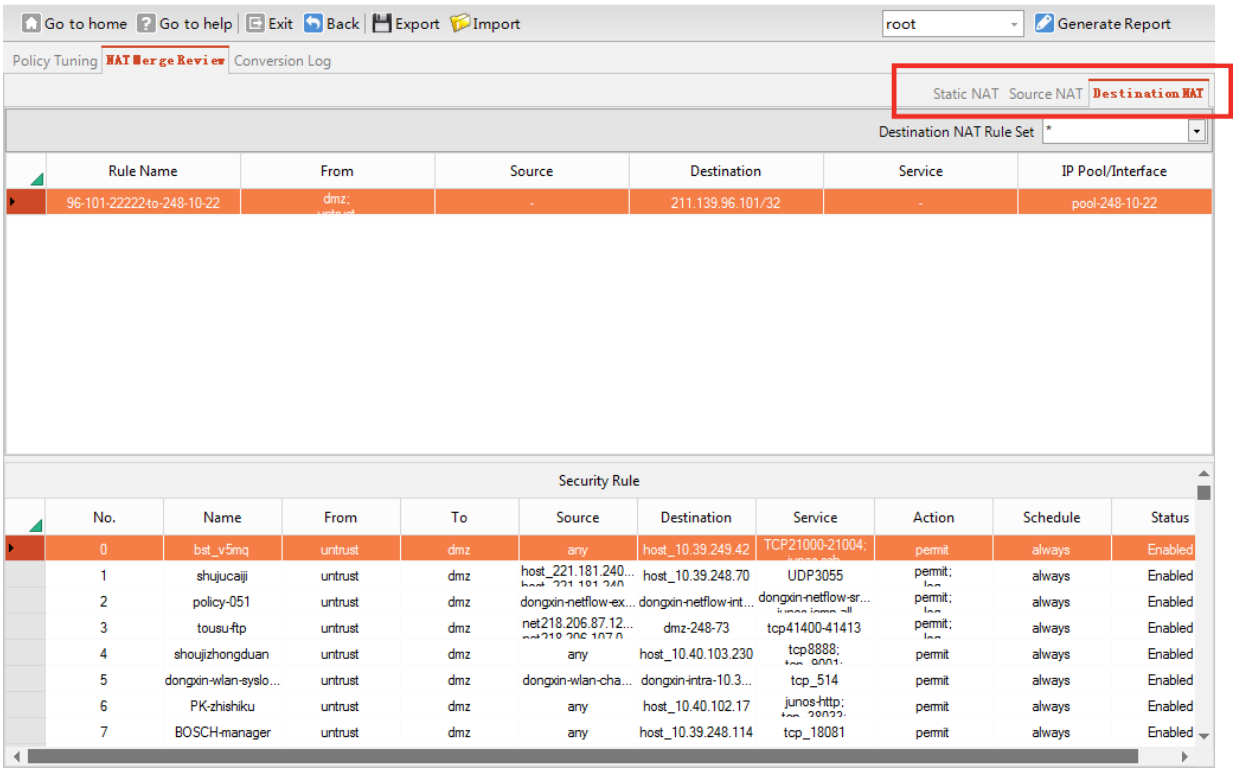
To reorder rows, click the policy number and drag the row to the new position.

## NAT Merge Review tab

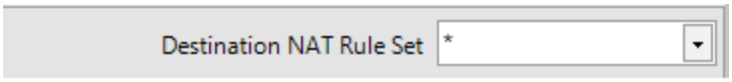
Currently, the NAT Merge Review tab allows you to review the NAT policy conversion logic for Juniper Junos OS and Check Point conversions only.

### Junos NAT Merge Review

You can use the sub-tabs in the top-right corner to select the NAT category to display Source NAT, Destination NAT, Static NAT, Object NAT, Double NAT, and NAT Rule. The source configuration determines which categories are available.

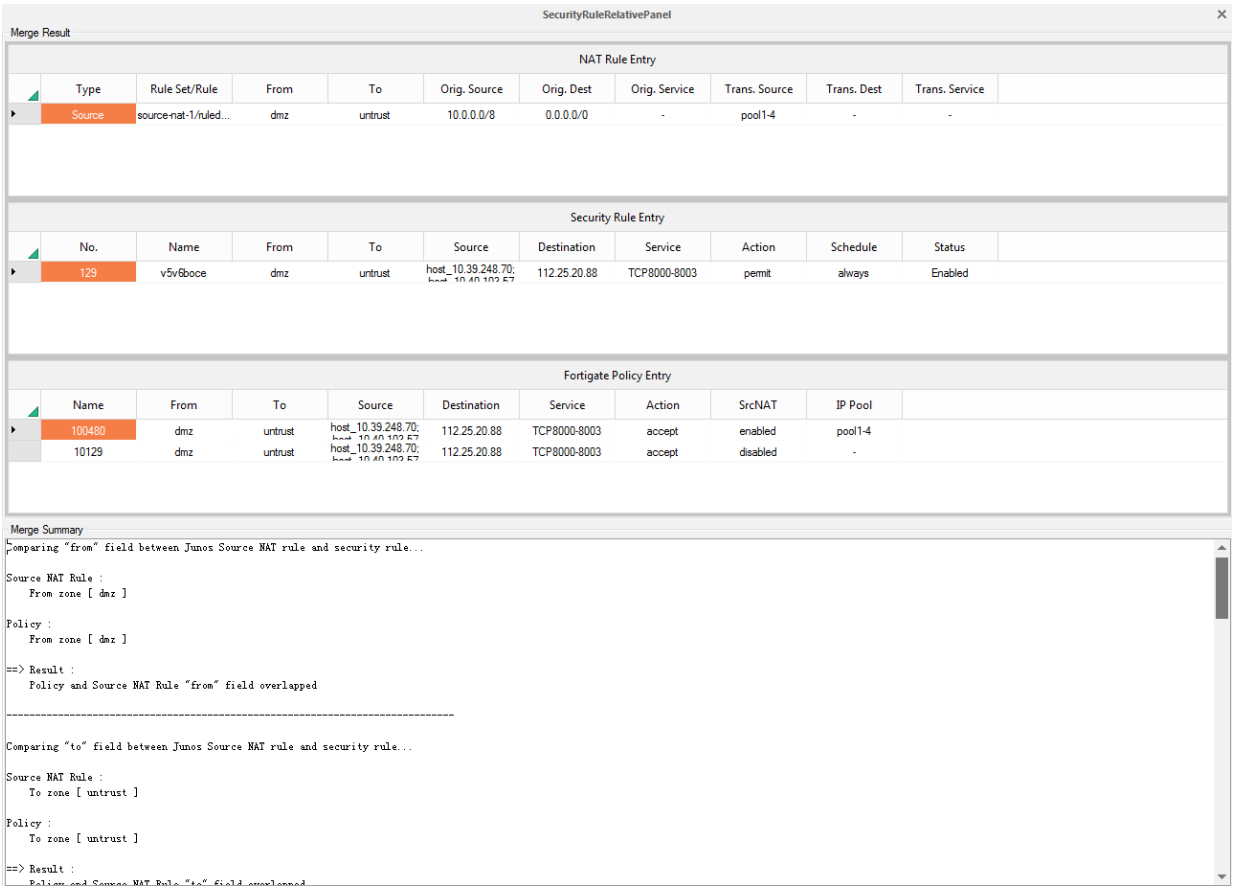



To display a particular rule set from the source configuration, for **Destination NAT Rule Set**, select the appropriate value.




The top pane of the NAT Merge Review tab is a list of NAT rules from the source configuration. Double-click a NAT rule to display the corresponding items in the Security Rule list (bottom pane).

Double-click a security rule to open the Merge Result window.




The Merge Result window displays the NAT rule, the security rule, and the resulting FortiGate policies.

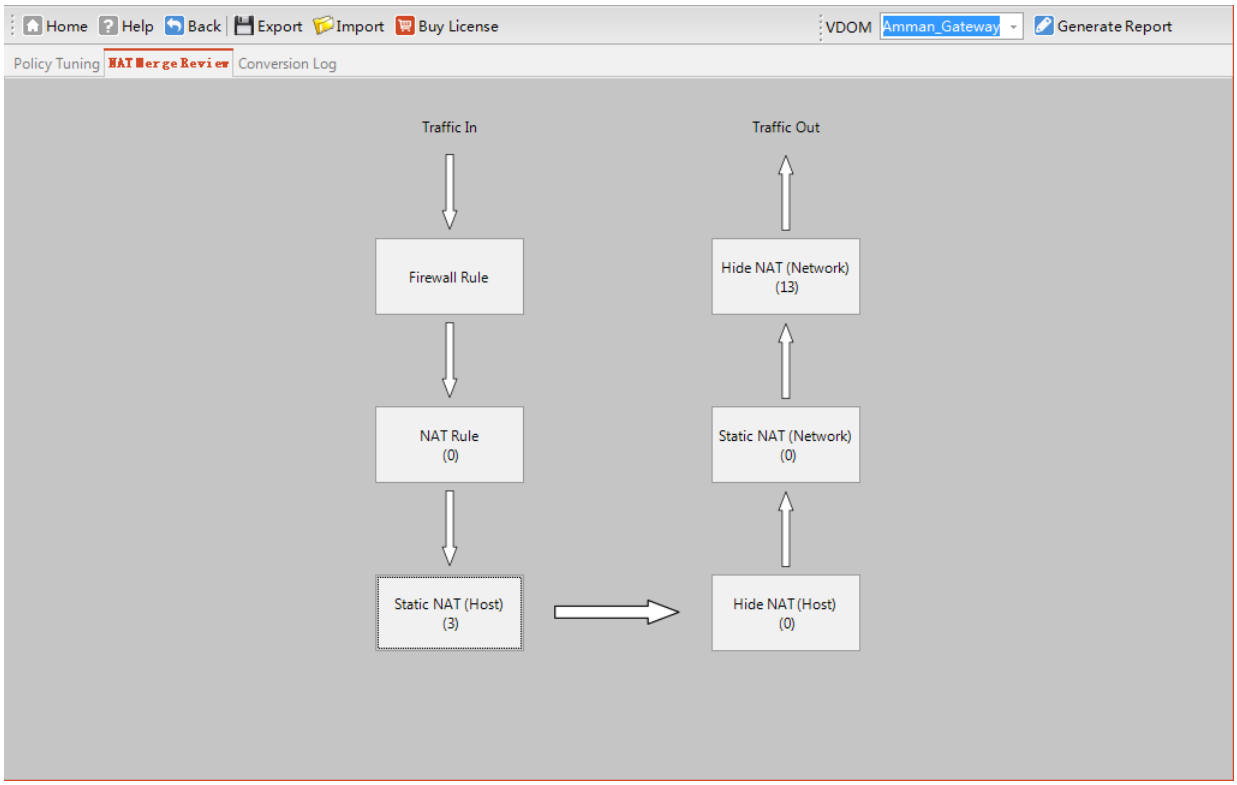
Policies that FortiConverter generated from a security rule from the source configuration have a five-digit name that is 10000 or higher .

Policies that FortiConverter generated by merging a NAT rule and security rule from the source configuration have a six-digit name that is 100000 or higher.

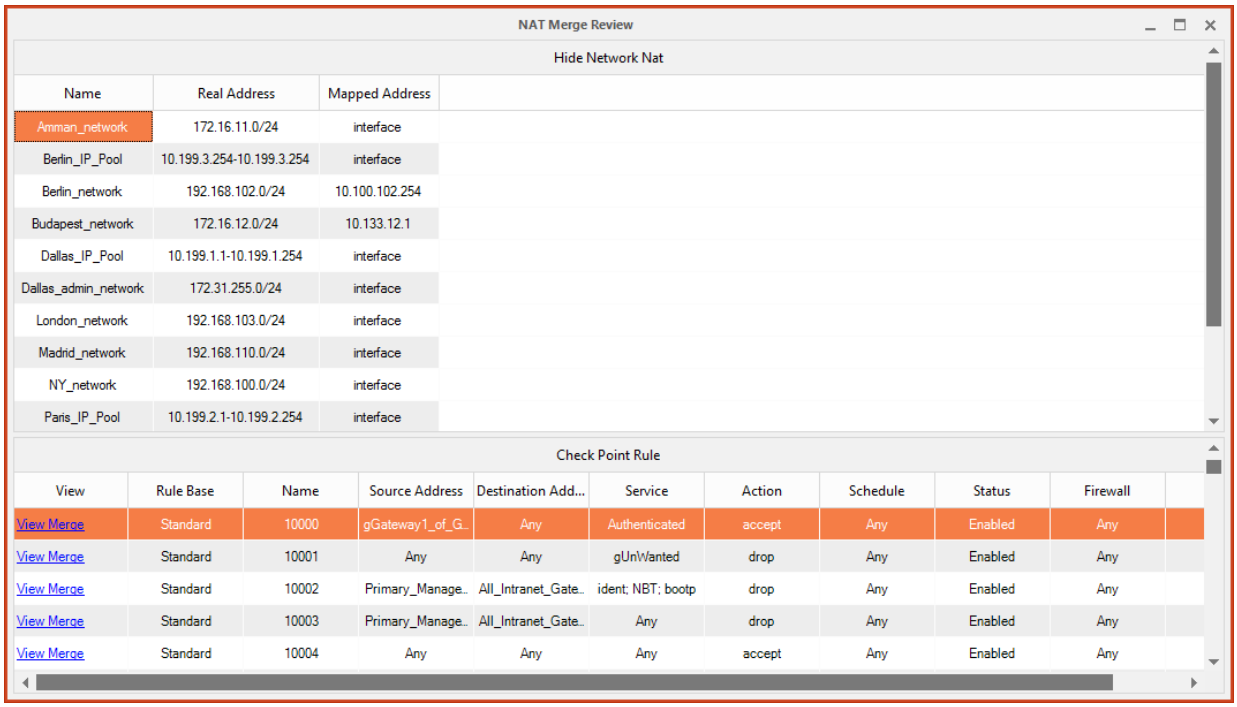
The Merge Summary provides a step-by-step description of the merge logic.

## Check Point NAT Merge Review

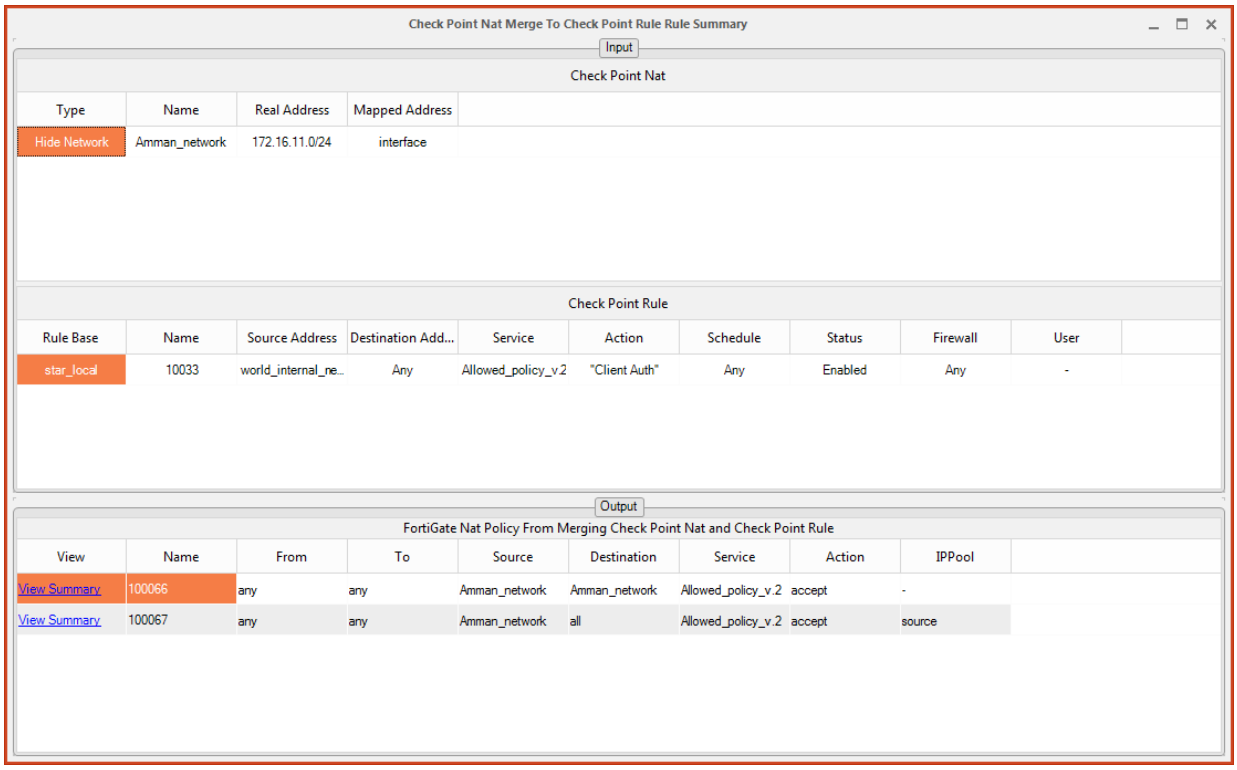
For Check Point, the NAT merge review tab displays the different NAT types as tiles in a diagram.



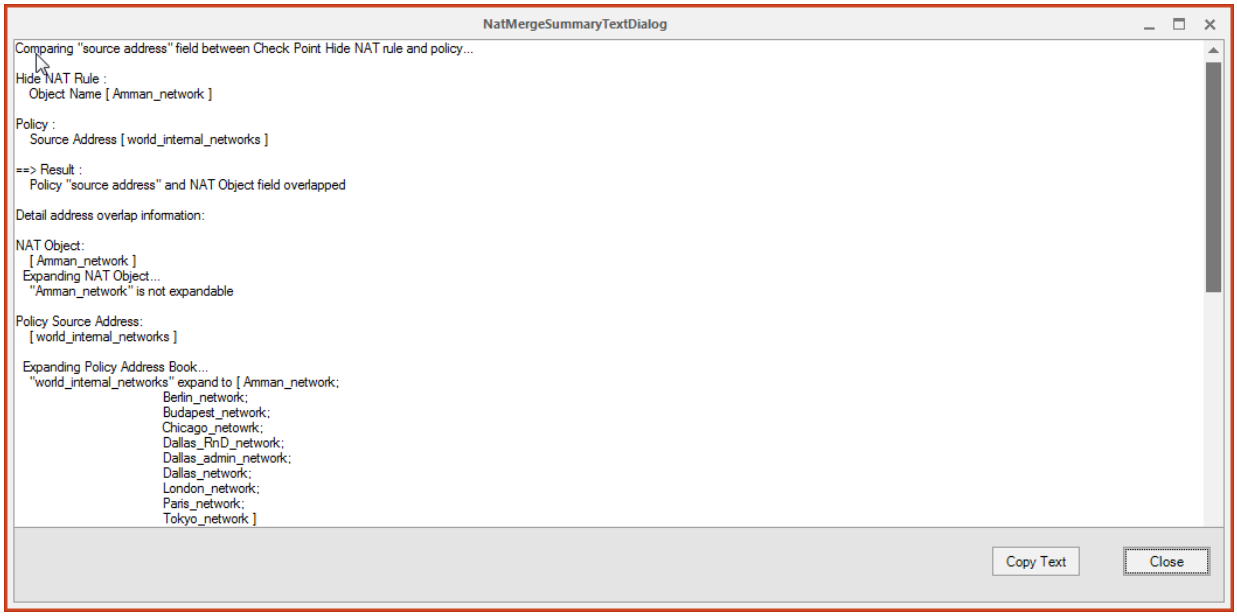

Click a tile to access the NAT rules and merge logs for that NAT type.




Click a network name, and then click **View Merge** to display detailed information about the input and output rules.

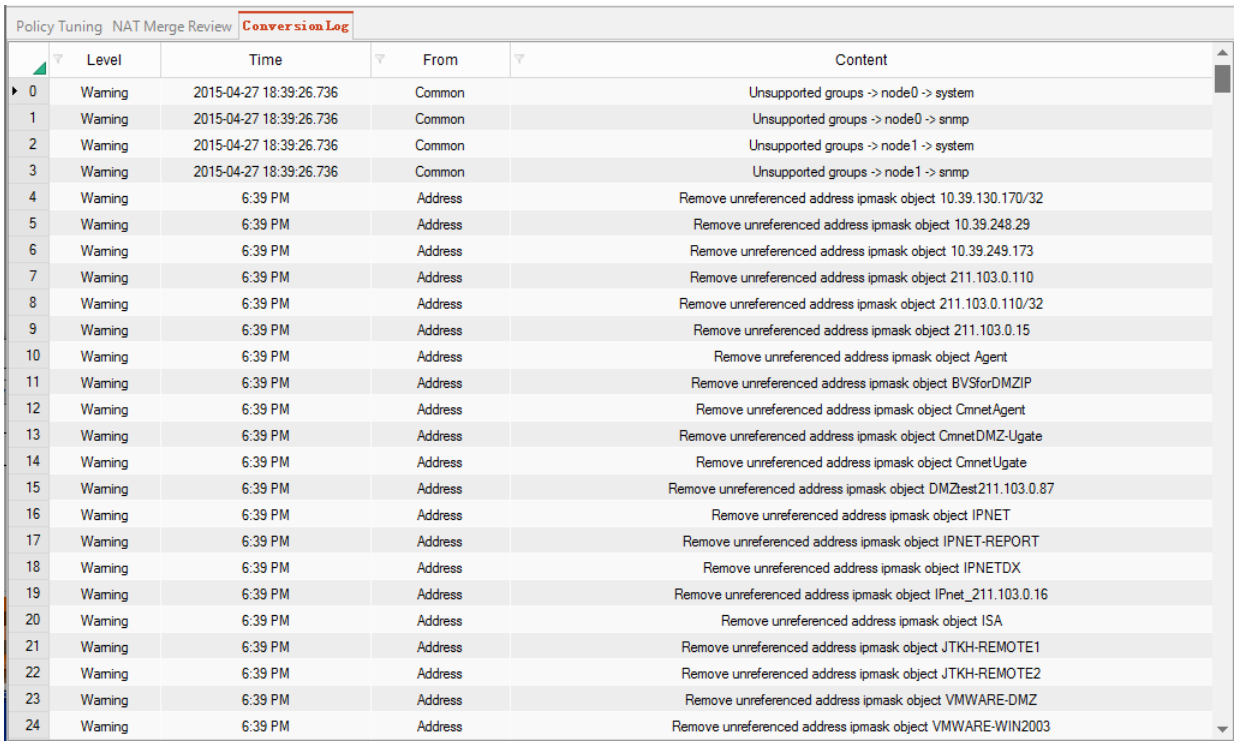



To view conversion log information about the merge, click **View Summary**.




## Conversion log tab

The Conversion Log tab displays warnings that FortiConverter generated during the conversion process.



Policy Tuning | NAT Merge Review | Conversion Log

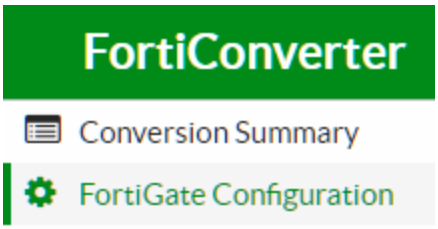
| | Level | Time | From | Content |
|---|---|---|---|---|
| 0 | Warning | 2015-04-27 18:39:26.736 | Common | Unsupported groups -> node0 -> system |
| 1 | Warning | 2015-04-27 18:39:26.736 | Common | Unsupported groups -> node0 -> snmp |
| 2 | Warning | 2015-04-27 18:39:26.736 | Common | Unsupported groups -> node1 -> system |
| 3 | Warning | 2015-04-27 18:39:26.736 | Common | Unsupported groups -> node1 -> snmp |
| 4 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object 10.39.130.170/32 |
| 5 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object 10.39.248.29 |
| 6 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object 10.39.249.173 |
| 7 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object 211.103.0.110 |
| 8 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object 211.103.0.110/32 |
| 9 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object 211.103.0.15 |
| 10 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object Agent |
| 11 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object BVSforDMZIP |
| 12 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object CmnetAgent |
| 13 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object CmnetDMZ-Ugate |
| 14 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object CmnetUgate |
| 15 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object DMZtest211.103.0.87 |
| 16 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object IPNET |
| 17 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object IPNET-REPORT |
| 18 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object IPNETDX |
| 19 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object IPnet_211.103.0.16 |
| 20 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object ISA |
| 21 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object JTKH-REMOTE1 |
| 22 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object JTKH-REMOTE2 |
| 23 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object VMWARE-DMZ |
| 24 | Warning | 6:39 PM | Address | Remove unreferenced address ipmask object VMWARE-WIN2003 |

# New application tuning

Although FortiConverter attempts to automatically convert as much of the source configuration as possible, in some cases, your input is required to complete the conversion. You will be automatically brought to the tuning page after your conversion completes.

**To make adjustments to your conversion:**

1. Click on **FortiGate Configuration**, located on the left.




2. Select one of the options that appear.

**To edit an existing object in your configuration:**

1. Double-click that row in the table.
   A dialog box will pop up.
2. Complete the fields as required, then click **OK**.

**To add or delete an object:**

1. Use the buttons located at the bottom of the page.


**To copy an object's CLI configuration:**

1. Click **Copy CLI**.


   A CLI Display box will pop up.
2. Click the Save icon to save the configuration as a text file, or click the Copy icon to copy the configuration to the clipboard.

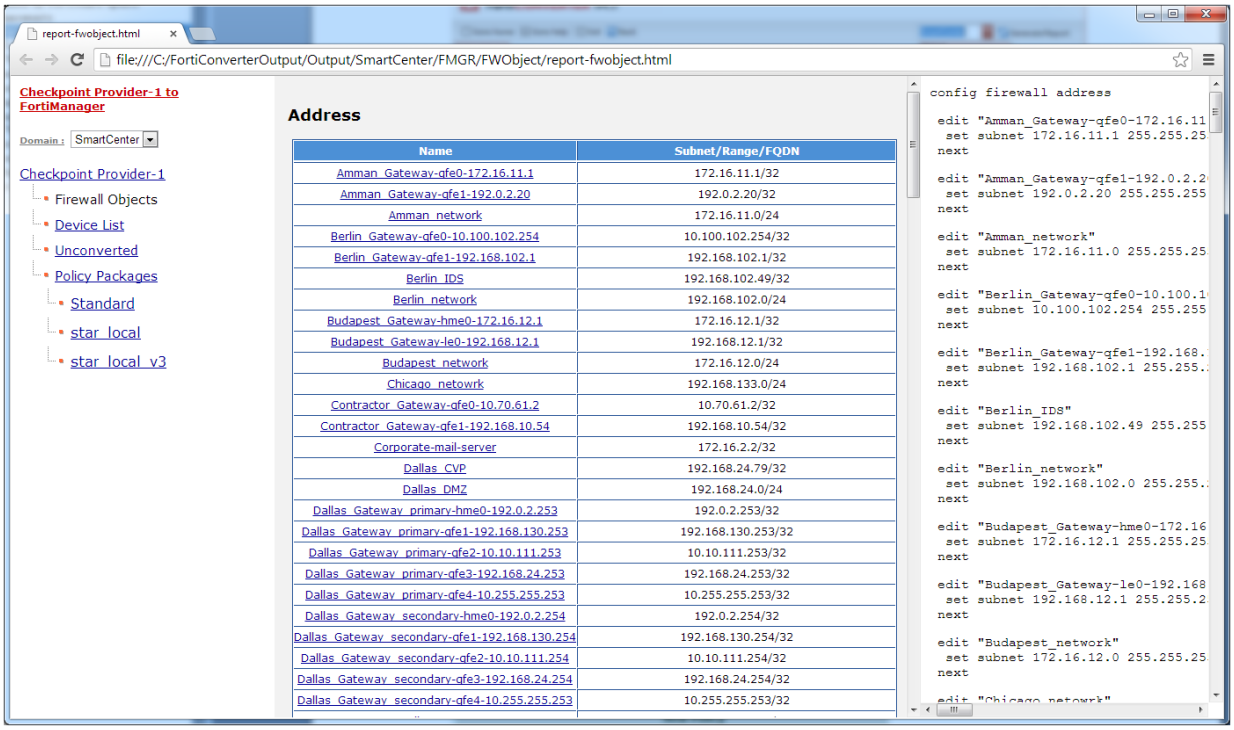
# Viewing the results of your automatic conversion

## Legacy application

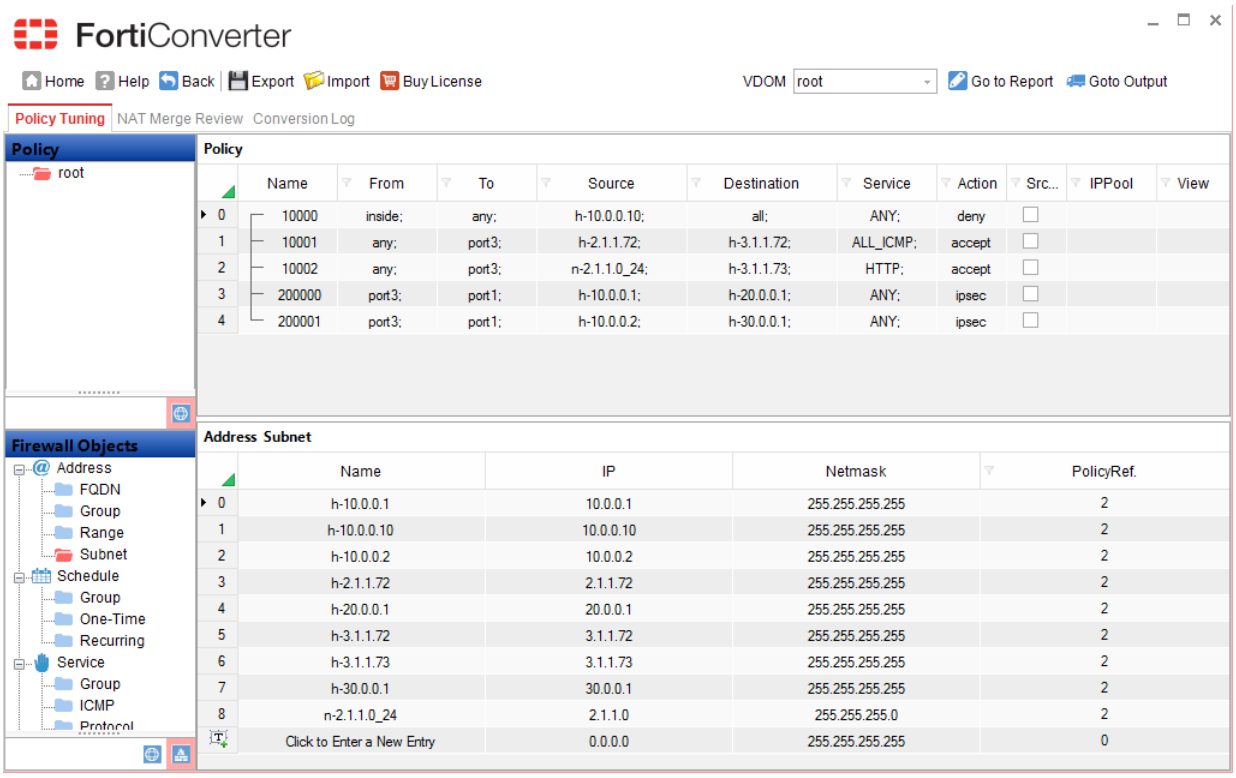
The Conversion Result page displays general conversion information, statistics on of the number of converted objects and policies, and a log of items that need further attention.

To see a summary of the conversion, click **Go to Report**.

An HTML page generated by FortiConverter is displayed in your web browser.




To examine the converted objects and policies in detail, click **Go to Tuning**. A window that allows you to tune the output is displayed.




After your review and any tuning tasks are complete, click **Go to Output** to access the final, converted configuration files.

## New application

The Conversion Summary page displays a summary of the conversion, including VDOM mapping and Interface mapping, as well as a device summary.

To fine-tune the conversion, click **FortiGate Configuration** from the menu on the left, then select an option.

To download the final, converted configuration files, click **Download Configurations**, located on the right.

**NOTE:** Configurations can also be downloaded from the home page by clicking the Download icon.

# Error messages

If an error occurs, FortiConverter inserts error messages and warnings into the conversion output file `config-all.txt`.

**NOTE:** These warnings are not inserted in the separate configuration branch files.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected.

## Undefined objects

```
# Error: Undefined interface/address/service/ippool object <NAME>
```

This error occurs when an object used in the policy is not previously defined. Make sure the object name is correct.

## Interface

```
# Warning: please input vlan interface
```

This warning is shown when the physical interface of a vlan interface is not specified.

## Zone

```
# Warning: Interface exists in other Zone.
```

This warning appears when an interface belongs to two zones at once. An interface should not belong to more than one zone at a time.

## Service

```
# Error: The number of service custom is <NUMBER>, exceed <NUMBER> limitation.
```

The number of services exceeds the maximum number supported by the selected FortiGate model.

## Service group

```
# Error: Unconverted members in service group <NAME>
```

This error occurs when objects in the mentioned service group are not converted and the service group becomes empty.

## User

```
# Warning: Cannot support radius server group
```

This warning is shown when the source configuration contains a radius server group. FortiGate does not support radius server groups. This warning only appears in Check Point conversions.

```
# Warning: Cannot find out radius server
```

This warning is shown when the radius server of the user is not defined in the source configuration. This warning only appears in Check Point conversions.

```
# Warning: please reset the shared secret key.
```

This warning appears when the password in the source configuration is encrypted. Reset the shared secret key.

## VIP

```
# Warning: Public IP confliction for below objects.
```

This warning appears when different VIP objects have the same public IP. Different VIP objects should not have the same public IP in FortiOS. To fix this issue, add port forwarding or source filter information to the conflicted VIP object.

## VPN phase1

```
# Warning: <NAME> exceed 35 characters"
```

This warning appears when a Phase1 name exceed 35 characters. To fix this issue, fix the name manually.

```
# Warning: remote-gw should be IP address, object <NAME> was not defined
```

This error occurs when the source configuration provides an address name for the remote-gw field. The remote-gw field should be an IP address.

```
# Warning: please reset the pre-shared key.
```

All the pre-shared keys are set to "123456" in the converted VPN object if the password in source config is encrypted. Users should reset the pre-shared keys.

## VPN phase2

```
# Warning: <NAME> exceed 35 characters
```

This warning appears when a Phase2 name exceed 35 characters. To fix this issue, fix the name manually.

## Policy

```
# set utm-status enable
```

```
# set application-list NAME1 NAME2
```

```
# Application-list support only one item, please recheck config file.
```

This error occurs when there are multiple items in the application list. There should be only one item in the application list. If there are multiple items given in the source configuration, reset the items.

```
# Warning: Removed self traffic object <NAME> from address list
```

```
# Warning: Comment out self traffic policy - object name <NAME>
```

Check Point policies may contain "self traffic" policies, but those policies are not needed in FortiOS.

```
# Warning: Comment out default drop all policy
```

There may be a "drop all" policy in the end of the policy list for some vendors. But FortiOS has its own "drop all" policy by default, so the one in source configuration should be commented out.

## Route static

```
# Warning: please input field <device>
```

The "device" (interface) route field is necessary in FortiOS.

## Snmp sysinfo

```
# Warning: Community <NAME> has <NUMBER> hosts, beyond the limitation
<NUMBER>.
```

The number of hosts in a community exceeds the maximum number supported by the selected FortiGate model.

## Other warnings

### Name length

```
# Warning: truncate <OBJECT> name <NAME> to <NUMBER> characters
```

```
# Warning: Trim <NAME> to <NUMBER> characters
```

When FortiConverter detects an object name that is longer than the limit given in FortiOS, FortiConverter will rename the object.

### Route BGP

```
# Warning: please reset the password.
```

This warning appears when the password of route BGP neighbors in the source configuration is encrypted. Reset the password of the route BGP neighbors.

### Route OSPF

```
# Warning: please reset the md5 key.
```

This warning appears when the md5 key of the OSPF interface in the source configuration is encrypted. Reset the md5 key.

# Importing your new configuration into FortiGate

### Conversion to FortiGate output

When you convert a source configuration to a FortiGate configuration, FortiConverter puts the conversion result in your output directory's FGT/ folder. This folder contains the conversion reports in HTML and the CLI configuration in the text file `config-cmd.txt`.

The `config-cmd.txt` file header contains basic import instructions. The converted objects and polices are located after the header and can consist of several thousand lines of configuration.

### Preparing the output configuration file for import

Before you import the output configuration, search the file for any comments that indicate issues that FortiConverter detected during the conversion (such as missing objects or conflicting object values) and fix them. To locate these comments, search for lines that start with `#` (number/hash symbol). You cannot successfully import the configuration if you do not fix these issues.

Fortinet recommends that you divide the configuration into sections, and then import one section at a time. If a section is large, divide it into smaller sections.

### Importing the configuration file sections

To import the sections of the output configuration file, Fortinet recommends that you use the **Upload Bulk CLI Command File** option at one of the following locations:

- **System > Config > Advanced** (FortiOS 5.2)
- **System > Advanced** (FortiOS 5.4 and 5.6)

Because you cannot successfully import a section of configuration that references an object that does not already exist in the configuration, ensure that you import the configuration sections in their original order. For example, you typically import polices last because they reference interfaces, addresses, users, services, IPsec phase1s, security policies, and so on. If these objects are missing, FortiGate does not accept the policy.

### CLI debugging

To make troubleshooting easier when there are import errors, before you import sections, enable CLI debugging.

By default, CLI debugging is level 3. This is the level to use under normal conditions.

You can use the following command to view the current debug level:

```
# diagnose debug info
```

A response similar to the following information is displayed:

```
debug output: disable
console timestamp: disable
console no user log message: disable
CLI debug level: 3
```

For the configuration importing process, the appropriate debug level is 8. Use the following command to change the debug level:

```
diag debug enable
diag debug CLI 8
```

When the import process is complete, use the following command to return the debug level to the default (3):

```
diag debug reset
```

### Importing process

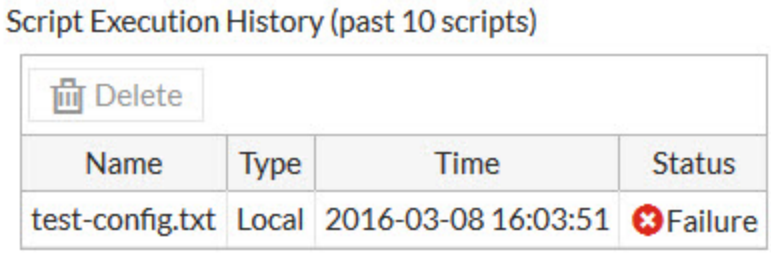
Import the sections of the conversion output systematically. For each section you import, check for import failures in the web UI Script Execution History. Use CLI debugging to diagnose and fix any errors. When the web UI indicated the import is completely successful, continue with the next section of the configuration.

### Example import error and troubleshooting

The following simple configuration generates an error because Test3 is not defined:

```
config firewall address
   edit "Test1"
      set subnet 1.1.1.1 255.255.255.255
   next
   edit "Test2"
      set subnet 1.1.1.2 255.255.255.255
   next
end
config firewall addrgrp
   edit "Test-Addresses"
      set member "Test1" "Test2" "Test3"
   next
end
```

When you save this configuration as a file and import it, the web UI displays the status Failure:



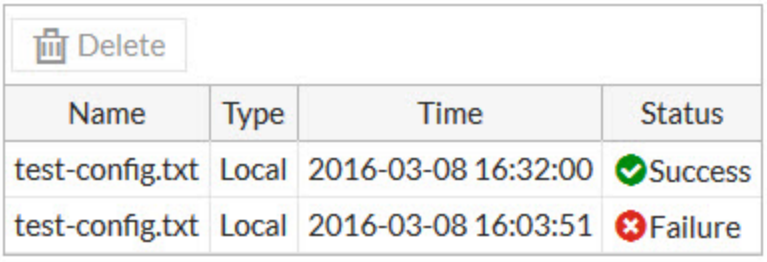

The following CLI output captures detailed information about the error:

```
0: config firewall address
0: edit "Test1"
0: set subnet 1.1.1.1 255.255.255.255
0: next
0: edit "Test2"
0: set subnet 1.1.1.2 255.255.255.255
0: next
0: end
0: config firewall addrgrp
0: edit "Test-Addresses"
-3: set member "Test1" "Test2" "Test3"
1: next
0: endwrite config file success, prepare to save in flash
```

The error code `-3` indicates that FortiGate did not find the object and the return code `1` indicates that an error occurred.

Notice that FortiGate creates the address objects Test1 and Test2. The failure status in the web UI only relates to the address group.

When you fix the script by adding the missing Test3 object and import it again, the web UI displays the status Success.




When the configuration is fixed, all the return codes in the CLI debugging are `0`, which indicates no errors.

```
0: config firewall address
0: edit "Test1"
0: set subnet 1.1.1.1 255.255.255.255
0: next
0: edit "Test2"
0: set subnet 1.1.1.2 255.255.255.255
0: next
0: edit "Test3"
0: set subnet 1.1.1.3 255.255.255.255
0: next
0: end
0: config firewall addrgrp
0: edit "Test-Addresses"
0: set member "Test1" "Test2" "Test3"
0: next
0: endwrite config file success, prepare to save in flash
```

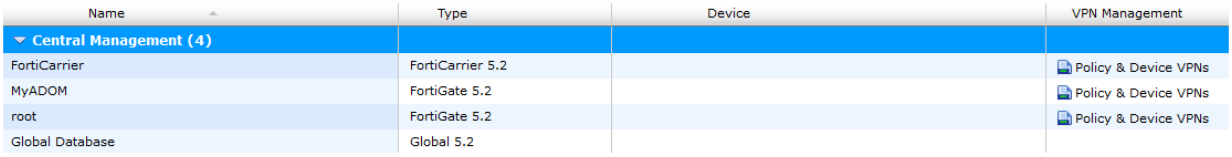
# Importing your new configuration into FortiManager

The example in the procedures uses FortiManager 5.2 and global policies and objects. The procedures are similar for environments that do not use the global feature.

### To configure FortiManager

On FortiManager, enable the ADOM feature and create an ADOM for each source domain that you want to migrate.

Ensure that all the ADOMs (including the global ADOM) use the same version of FortiOS.



| Name | Type | Device | VPN Management |
|---|---|---|---|
| Central Management (4) | | | |
| FortiCarrier | FortiCarrier 5.2 | | Policy & Device VPNs |
| MyADOM | FortiGate 5.2 | | Policy & Device VPNs |
| root | FortiGate 5.2 | | Policy & Device VPNs |
| Global Database | Global 5.2 | | |

### The output folder

The output folder provides both a global folder and a folder for each source domain. Both folders contain the subfolder `FMGR\`.

Object configuration is located in the `FMGR\FWObject\` folder, which contains the following files:

- Several text and HTML files that are used for reporting. They are not used to import the configuration.
- The text file `config-all` , which contains all the CLI commands for the object configuration.
- Text files that duplicate sections of the `config-all` file: `address`, `address groups`, `services`, `scheduled`, and so on. When there are many objects (for example, most environments have many firewall address objects), these sections are divided into multiple, indexed files. To make the import process simpler, Fortinet recommends that you import configurations using the files for individual sections.

Policy scripts are located in policy package folders in `\FMGR\Policy` as one or more firewall policy files (`config-firewall-policy-1`, `config-firewall-policy-2`, and so on).These files are the same content as the conversion output file `config-all` in smaller, indexed files that are easier to import.

### Running scripts

With the exception of `config-system-session-helper`, you run all scripts using the **Policy Package, ADOM Database** script target.

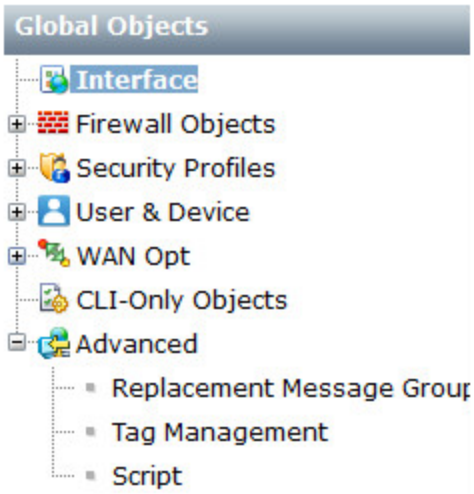
You run the `config-system-session-helper` script on the device database to set device-level settings.

If the global folder contains a `config-system-session-helper` script, review its contents. In most cases, it is not required because the global policies and objects configuration does not contain devices. You can add any configuration in this script to session helper scripts for each domain that uses the global objects. However, in most cases, the domain-level script also contains these settings.

### To import policies and objects

You import your global object and policies first because the ADOM configuration can depend on them. Import objects before policies because polices depend on objects.

1. In the FortiManager system settings, to enable scripts, go to **System Settings > Admin > Admin Settings**. Under **Display Options on GUI**, select **Show Script**.
2. To display the scripts in the Global Objects menu, on the Policy & Objects tab, go to **Tools > Display Options > All On**.
3. Go to **Global Objects > Advanced > Script**.



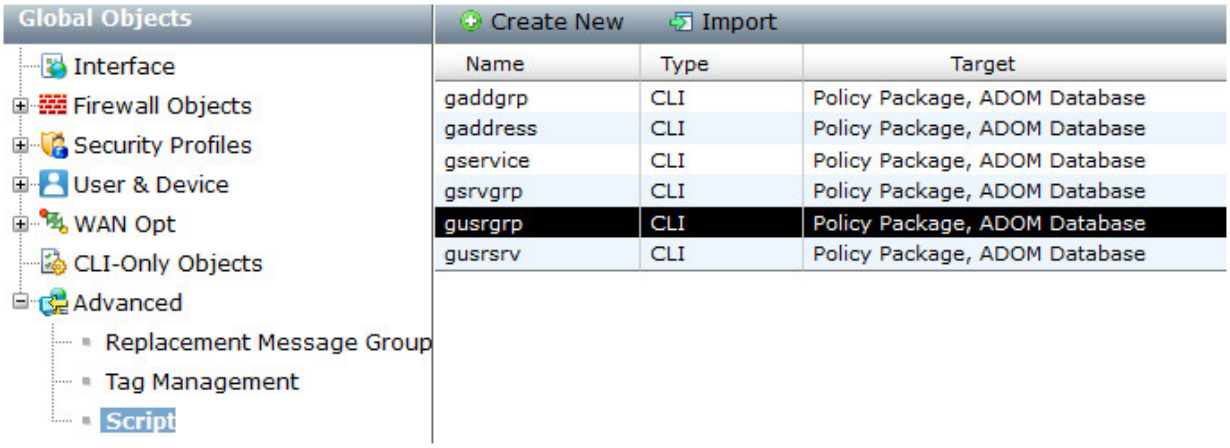

The list of global scripts is displayed.

4. Click **Import**, enter a name for the script you are importing, and then click **Browse** to navigate to and select a script from the `Global\FMGR\FWObject` folder.

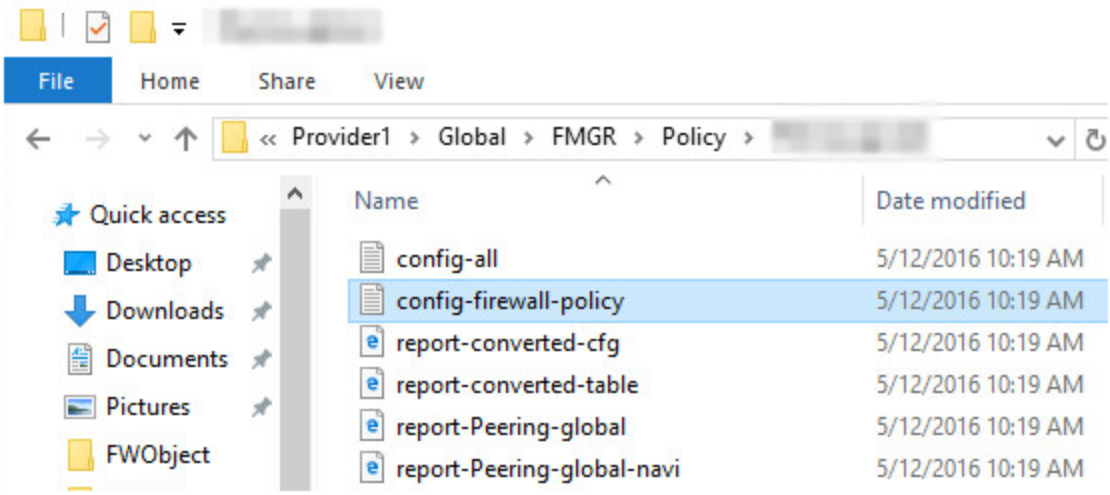
   For more information on the output folders and files, see The output folder on page 127.
5. For the script target, select **Policy Package, ADOM Database**, and then select **OK**.
6. When the import is complete, review any error messages that FortiConverter inserted as comments and make any required corrections. For more information, see To troubleshoot script import and execution errors on page 131.
7. To run the script, right-click it, and then select **Run**. Because global objects are applied to all ADOMs by default, for **Run script on policy package**, you can use the default policy package.

   If the script execution fails, troubleshoot the process and make any required changes. For more information, see To troubleshoot script import and execution errors on page 131.

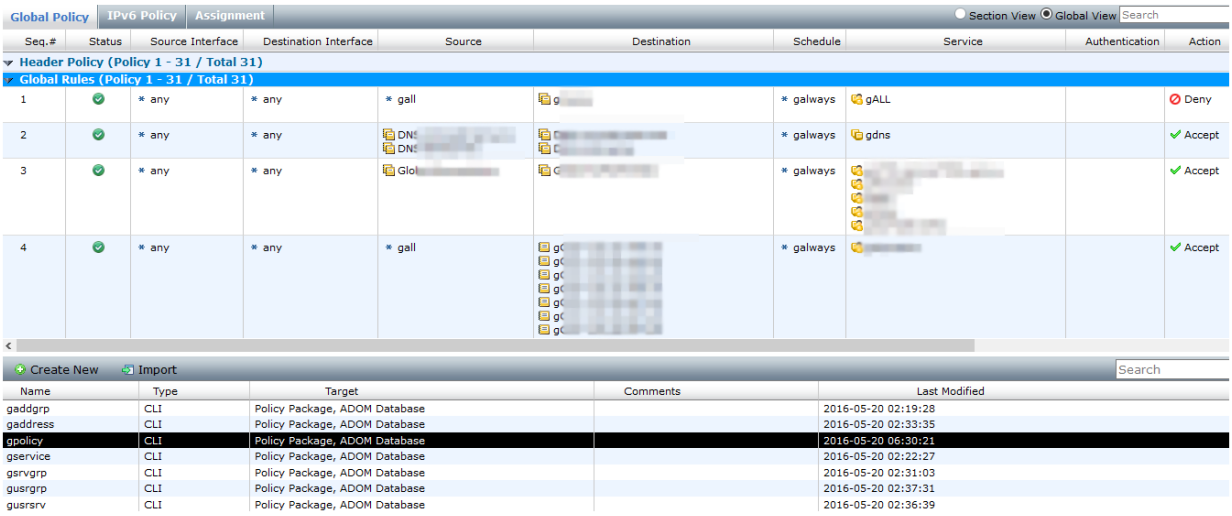
8. Repeat the script import and run process for all the scripts in the `Global\FMGR\FWObject` folder.



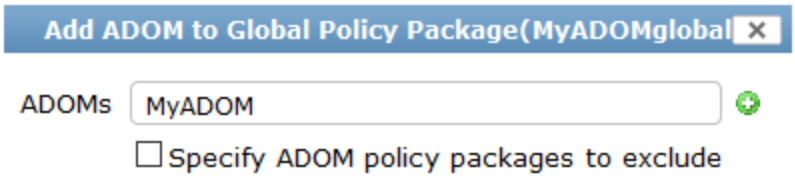

9. When you have imported all the objects, use the same procedures to import and run the policy scripts using the firewall policy configuration files located in the `Global\FMGR\Policy` folder, which contains a folder for each policy package. Do not import the `config-all` file.




After the scripts have run successfully, review the policies.

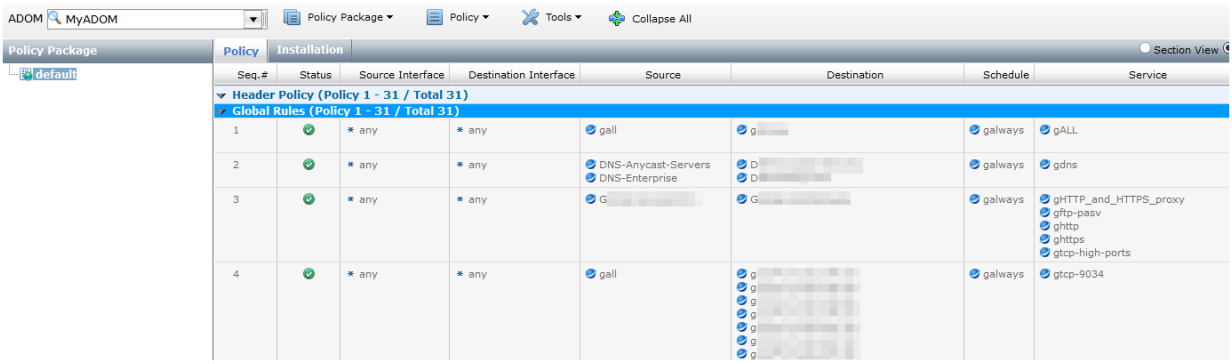



**10.** When the policy package is correct, assign it to your ADOM. By default, FortiManager assigns the selected policy package to all policy packages in the ADOM.




**11.** To complete the ADOM assignment, on the Assignment tab, click **Assign**.


**12.** When the process of assigning the polices and objects is complete, on the Policies & Objects tab, select the ADOM to review the policies.



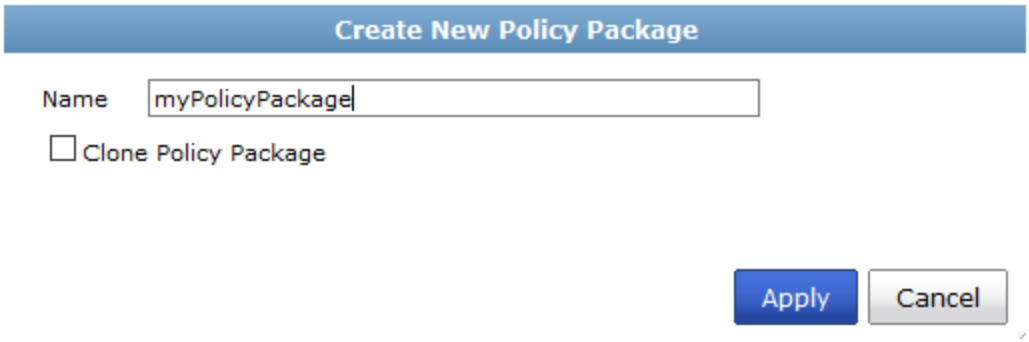

**13.** To import the domain-level polices and objects into your ADOM, on the Device Manager tab, select the ADOM, and then go to **Scripts > Script**.

14. Repeat the procedure for importing the object and policy scripts with the contents of the `<domain_name>\FMGR\FWObject` and `<domain_name>\FMGR\Policy` folders. Import the objects first.

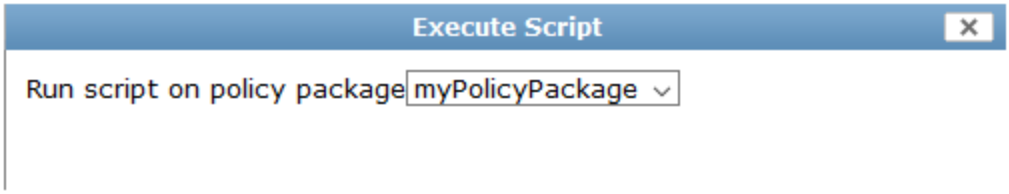
    Do not import the `config-system-session-helpers` script. For the script target, select **Policy Package, ADOM Database**.

    Ensure you check for error messages that FortiConverter inserted as comments and make any required corrections. For more information, see To troubleshoot script import and execution errors on page 131.
15. Run each imported object script. For **Run script on**, select **Policy Package, ADOM Database**. Correct any errors that prevent the script from executing. For more information, see To troubleshoot script import and execution errors on page 131.

    If there are many address objects, you import several scripts because the address file is indexed to keep the files at a manageable size. For more information, see Working with object output in indexed files on page 134.
16. Before you run the policy scripts, create new policy packages that correspond to each policy package folder in `<domain_name>\FMGR\Policy`. On the Policy & Objects tab, right-click on the default policy package and choose **Policy Package Create New**. Clear the **Clone Policy Package** option.




    Because global polices and objects were assigned to all policy packages in this ADOM, they are automatically part of each new policy package. The next import task adds the domain-level policies.
17. On the Device Manager tab, run each imported policy script. For **Run script on**, select **Policy Package, ADOM Database**. When you are prompted for a policy package, select the name of the appropriate package, which you created earlier.

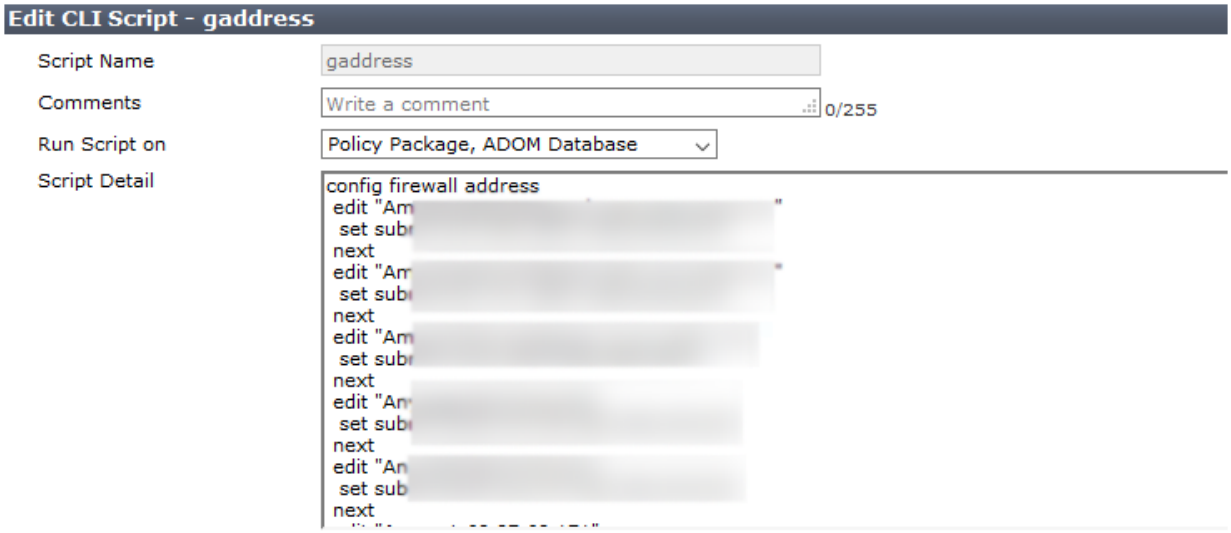



    Correct any errors that prevent the script from executing. For more information, see To troubleshoot script import and execution errors on page 131.

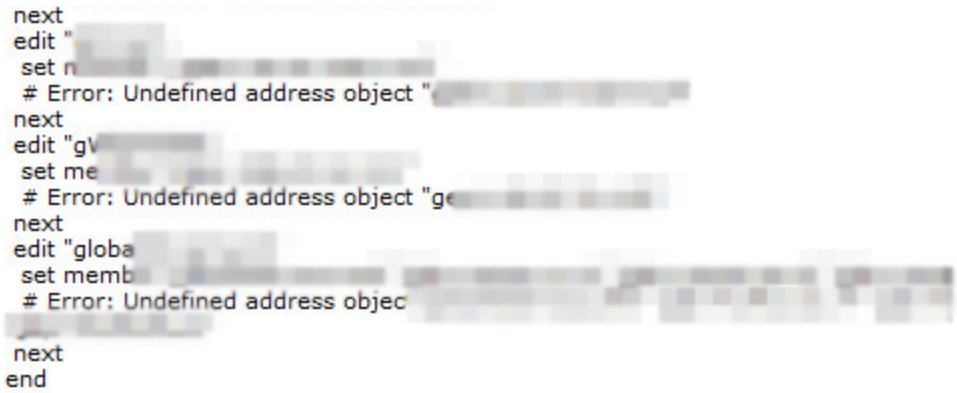
### To troubleshoot script import and execution errors

FortiConverter inserts any error messages in output scripts as comments.

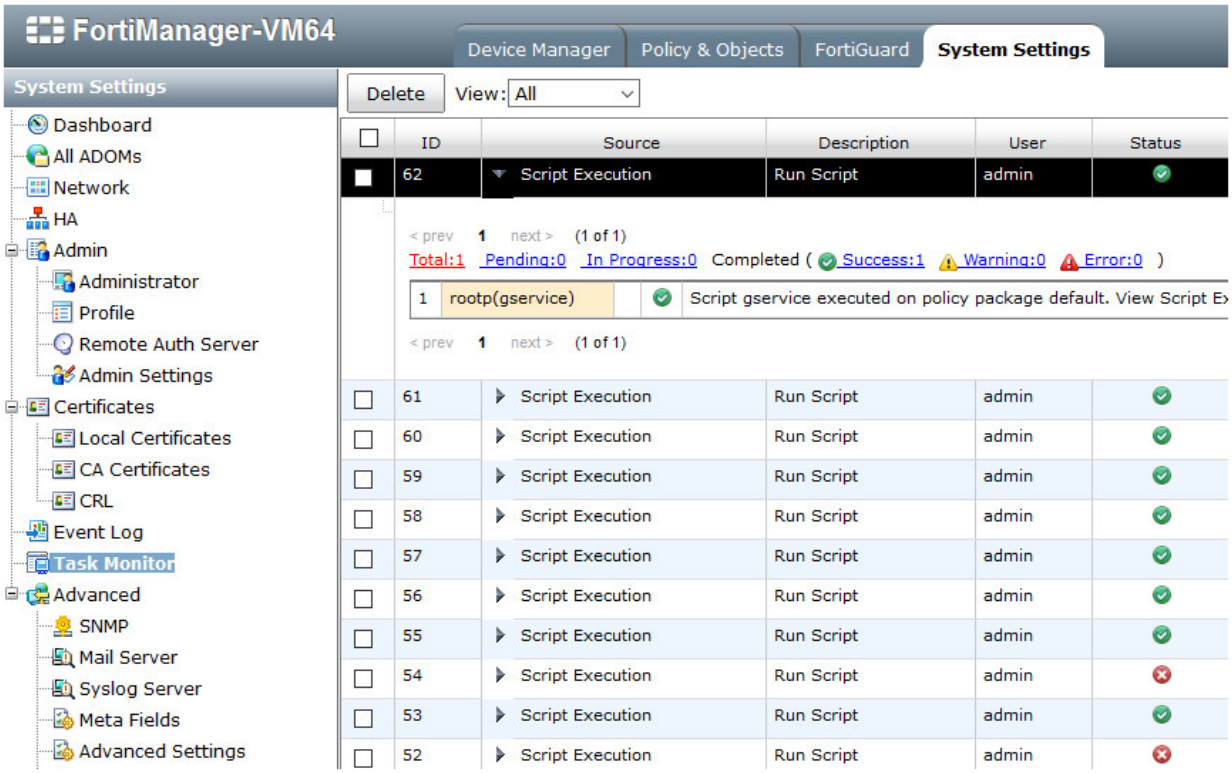
In some cases, the script cannot run unless you edit it to correct the errors. Double-click the name of the script in the list of scripts to edit it.




In the following example, the address objects that generate the errors are assigned using the global objects and can be ignored.




If an error occurs during script execution, go to **System Settings > Task Monitor** to view the error message and identify the error. Look for "Failed to commit to DB" in the task information.




Unlike a FortiGate import, which creates an object up to the point of failure, FortiManager creates no objects or policies if the script execution fails.

If you identify the cause, correct it in your script.

For example, the following error was generated by a firewall policy that contained both IPv4 and IPv6 objects, which FortiOS does not support and FortiConverter did not correct.

```
Failed to commit to DB, reason(command(set global header policy.1073741852:dstaddr "IP-1[redacted]" "IP-200[redacted]3")
Running script(gpolicy) on DB failed
------- The end of log ----------
```

Another example of a script execution error generates the following message:

```
edit "Con[redacted]
Failed to commit to DB, reason(syntax error)
Running script(address1) on DB failed
------- The end of log ----------
```

To resolve the error, determine which object precedes the error, locate it in the script, and correct any configuration errors. In this example, the configuration does not specify the subnet. If an object you do not want to use generates the error, you can delete it from the script or use # (hash) at the start of the appropriate lines to convert them to comments. Then, try to run the script again. Repeat the troubleshooting process until the script execution is successful.

If there is no obvious error in the output, try dividing the script into two smaller scripts. If only one script runs successfully, you have narrowed the focus of your troubleshooting to the content of the failed script. To divide a script, right-click it and select **Clone**. Using the policy numbers to determine and keep track of which policies you delete, edit the files so that they each contain a different section of the script. Then, run both scripts.

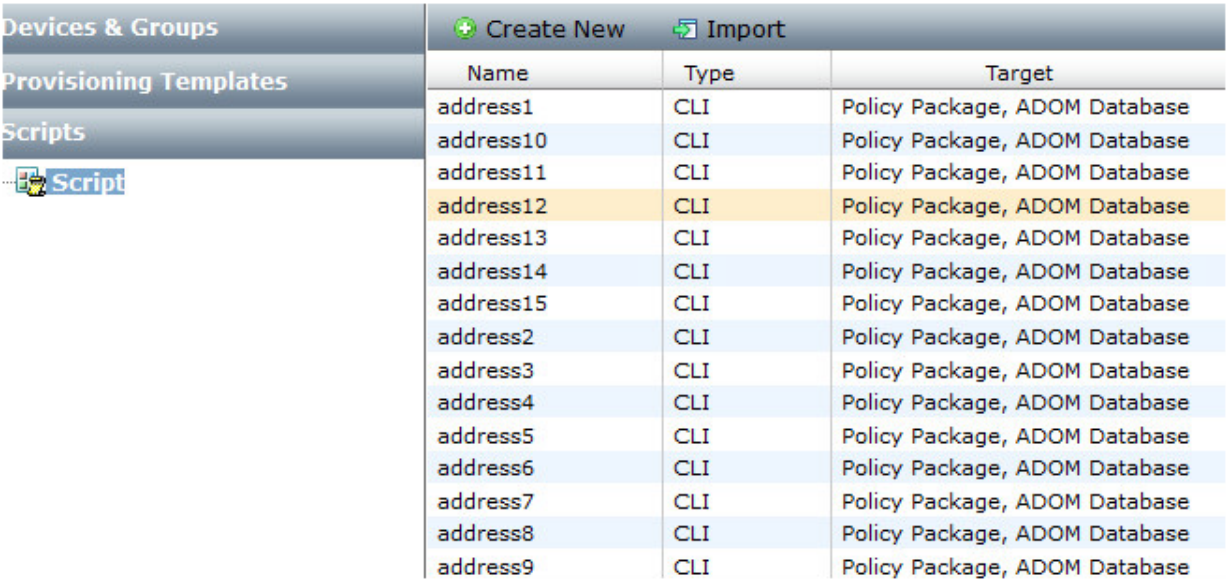
Dividing scripts into two or more smaller scripts is also useful if you suspect the length of a script is causing the execution to fail. Scripts that are too long fail without generating an error message.

In some cases, if a script fails, Fortinet recommends that you create a new script instead of editing or deleting it, because sometimes files can remain after you delete it. If you preserve the failed script, you can review it and the error it generates later. In the following example, the following `config user server` objects took several attempts to run successfully.

| | | |
|---|---|---|
| service1 | CLI | Policy Package, ADOM Database |
| service2 | CLI | Policy Package, ADOM Database |
| session-helper | CLI | Device Database |
| user-servera | CLI | Policy Package, ADOM Database |
| user-serverb | CLI | Policy Package, ADOM Database |
| user-serverc | CLI | Policy Package, ADOM Database |

### Working with object output in indexed files

In some cases, output files are split into smaller, indexed files to make it easier to import them.




If a configuration contains nested groups, script execution can fail because groups defined in one file are dependent on groups defined in another file.

If a script fails because of a missing dependency, remove the object that causes the failure. When you have finished importing the scripts for the object type, delete the script you edited and import it again. Then, run the script without editing it. Because the dependency is now included in the imported configuration, the unedited script can execute successfully.

# Troubleshooting



## Licensing

FortiConverter is a single-user application. Using more than one user account may invalidate the Hardware ID. If multiple users require the application, Fortinet recommends that you install it using a single, shared account, on a remotely accessible host.

A hardware layer change will generate a new hardware identifier. For a physical host, this could occur when installing the application on a new laptop, or installing a memory extension or a new network card. For a virtual host, such as VMware, the hardware identified may change because of an update in the virtualization software, or because of a change to the virtual hardware configuration for that virtual host.

Windows updates may on occasion affect the hardware id, particularly .Net framework updates.

If your license does change, please contact customer services, cs@fortinet.com, include your serial number, previous hardware identifier, and new hardware identifier. They will update your FortiCare records and you will be able to download the replacement license from the support portal.

## Accessing conversion logs

In most cases, when FortiConverter has an internal problem, the application displays a message in the web UI and adds an error message to a log file.

The logs capture all the conversion steps, including initialization, parsing (two logs), conversion, and reporting.

If the log indicates that FortiConverter encountered an internal error, or for help resolving other errors, contact the FortiConverter team at fconvert_feedback@fortinet.com.

### Log location

The logs are stored at the following default location (ProgramData is a hidden folder):

```
C:\ProgramData\Fortinet\FortiConverter\logs\<date>
```

where `<date>` is the day the log was generated. For example, `2016-04-25`.

### Example logs

Logs are plain-text files. These examples have additional formatting to illustrate the different steps and highlight errors.

### Successful Juniper ScreenOS conversion

Info:

2016-04-25 16:58:10.2853

MainWizardPanel.btnStart_Click => MainWizardPanelPresenter.Initialize => ConverterManager.MakeANewConversionJob

**Start a New Conversion: Juniper**

Info:

2016-04-25 16:58:17.6680

BackgroundWorker.OnDoWork => VdomWizardPresenter._vsysPhaseCallWorker_DoWork => VdomConvertJob.DoConvertForGetVDOM

**Parse VDOM:** C:\Users\user\Desktop\Test Case Base\ScreenOS\test_sos.txt

Info:

2016-04-25 16:58:18.8052

BackgroundWorker.OnDoWork => JuniperWizardPresenter._firstPhaseCallWorker_DoWork => ConvertJob.DoConvertForFirstPhase

**Parse:** C:\Users\user\Desktop\Test Case Base\ScreenOS\test_sos.txt

Info:

2016-04-25 16:58:22.7495

BackgroundWorker.OnDoWork => VdomWizardPresenter._secondPhaseCallWorker_DoWork => ConvertJob.DoConvertForSecondPhase

**Convert**

Info:

2016-04-25 16:58:23.6636

ConvertJob.DoConvertForSecondPhase => ConvertJob.DoConvertForThirdPhase => ConvertJob.DoConvertReportPartial

**Report: FGT**

### Failed Cisco conversion

The error message at the end of this example log indicates that FortiConverter encountered an internal error.

Info:

2016-03-29 18:59:33.8553

MainWizardPanel.btnStart_Click => MainWizardPanelPresenter.Initialize => ConverterManager.MakeANewConversionJob

**Start a New Conversion: Cisco**

Info:

2016-03-29 18:59:41.3151

BackgroundWorker.OnDoWork => VdomWizardPresenter._vsysPhaseCallWorker_DoWork => CiscoConvertJob.DoConvertForGetVDOM

**Parse VDOM:** C:\Users\user\Desktop\test_cisco.txt

Info:

2016-03-29 18:59:48.5378

BackgroundWorker.OnDoWork => CiscoWizardPresenter._firstPhaseCallWorker_DoWork => CiscoConvertJob.DoConvertForFirstPhase

**Parse:** C:\Users\user\Desktop\test_cisco.txt

Info:

2016-03-29 19:00:00.0919

BackgroundWorker.OnDoWork => MainWizardPanelPresenter._secondPhaseCallWorker_DoWork => ConvertJob.DoConvertForSecondPhase

**Convert root**

**Error:**

2016-03-29 19:00:38.1278

InterfaceALL.UpdatePolicyReference => InterfaceCollection.UpdatePolicyReference => PolicyOrg.HasReferencedInterface

**Reference interface failed: Object reference not set to an instance of an object.**

## Troubleshooting application crashes

In many cases, disabling NAT merge options can resolve an application crash that occurs during a conversion.

For example, for a Cisco PIX conversion, on the wizard's Start Option page, click **More**, and then for each type of NAT, select **Off**.

You can use the FortiConverter logs to access detailed information about the cause of a crash. See Accessing conversion logs on page 135.

## Reviewing errors in a restorable FortiGate configuration

When you select the wizard's **Create a restorable config** option, FortiConverter creates a config file by appending the converted source configuration to the target default configuration.

The output also includes any unconverted configuration items and errors, which you can review using the `config-error-log` CLI command.

```
diagnose debug config-error-log read
>>>  "set" "dlp-sensor" "[redacted]" @ 7717:firewall.policy.101000:value parse error (error -3)
>>>  "set" "dlp-sensor" "[redacted]" @ 7732:firewall.policy.102000:value parse error (error -3)
>>>  "set" "dlp-sensor" "[redacted]" @ 7747:firewall.policy.103000:value parse error (error -3)
>>>  "set" "dlp-sensor" "[redacted]" @ 7762:firewall.policy.104000:value parse error (error -3)
>>>  "set" "dlp-sensor" "[redacted]" @ 7777:firewall.policy.105000:value parse error (error -3)
>>>  "set" "dlp-sensor" "[redacted]" @ 7792:firewall.policy.106000:value parse error (error -3)
>>>  "set" "dlp-sensor" "[redacted]" @ 7807:firewall.policy.107000:value parse error (error -3)
>>>  "set" "dlp-sensor" "[redacted]" @ 7824:firewall.policy.108000:value parse error (error -3)
>>>  "set" "dlp-sensor" "[redacted]" @ 7839:firewall.policy.149000:value parse error (error -3)
>>>  "set" "dlp-sensor" "[redacted]" @ 7854:firewall.policy.149999:value parse error (error -3)
```

In many cases, one failed object causes many lines of output because the configuration uses it in multiple places.

The error log provides a line number that helps you to locate a command associated with the problem. To help you understand the problem, try entering the command in the CLI.

In the example, because of significant configuration changes since FortiOS 4.2, FortiConverter does not migrate Data Leak Prevention (DLP) settings from 4.3 to 5.2 and instead records the errors.

Common errors include the following codes:

- `-651` – Input value error. The CLI command is incorrect.
- `-3` – Entry not found (see the illustration). The value given, such as a profile name, is not configured..

# Appendix

## Adjusting table sizes

The conversion wizard Start Options page allows you to specify whether FortiConverter allows larger table sizes and group membership than default in the output configuration.

This is useful when, for example, the source configuration has a large address group and the target configuration can accommodate the larger group. Otherwise, FortiConverter converts the large address group into two or more smaller address groups for a single policy.

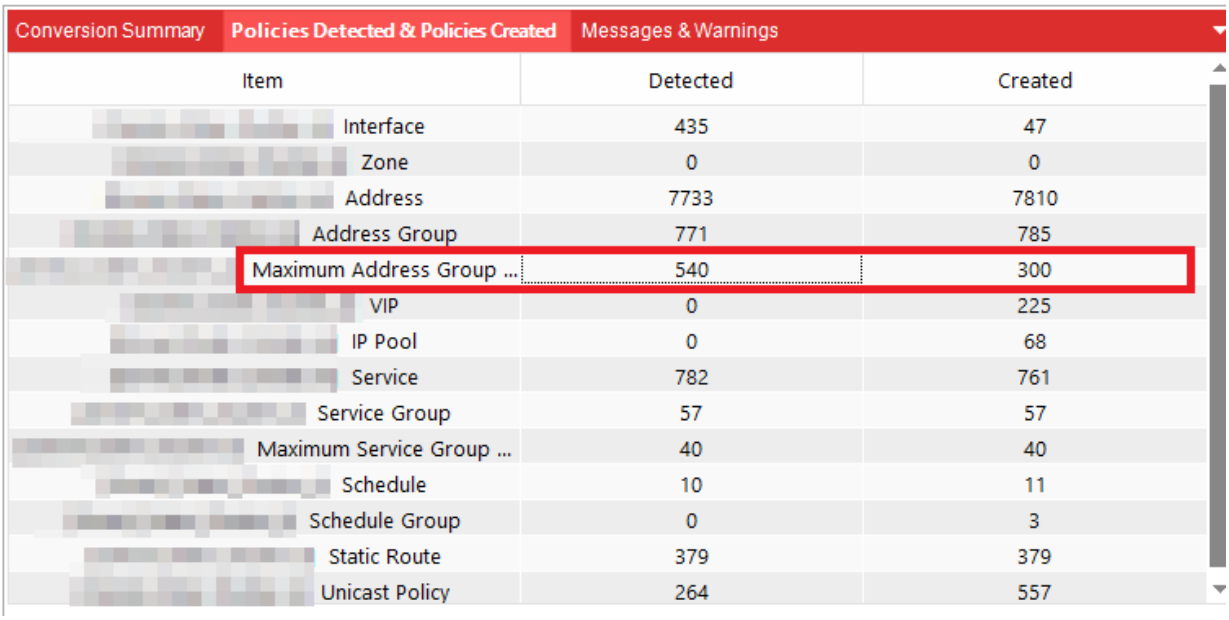
For example, FortiConverter uses the following default maximum table sizes by default:

- **Address groups** – 2500
- **Addresses per group** – 300
- **Custom service objects** – 1024

When this option is selected, FortiConverter uses the following maximum table sizes:

- **Address groups** – 20000
- **Addresses per group** – 1500
- **Custom service objects** – 4096

In the following graphic you can see the output has created address groups with a limit of 300 members, but the source config has instances with over 500 members. In this case you can increase the address group membership limit if the target device supports the higher value.




| Item | Detected | Created |
|---|---|---|
| Interface | 435 | 47 |
| Zone | 0 | 0 |
| Address | 7733 | 7810 |
| Address Group | 771 | 785 |
| Maximum Address Group ... | 540 | 300 |
| VIP | 0 | 225 |
| IP Pool | 0 | 68 |
| Service | 782 | 761 |
| Service Group | 57 | 57 |
| Maximum Service Group ... | 40 | 40 |
| Schedule | 10 | 11 |
| Schedule Group | 0 | 3 |
| Static Route | 379 | 379 |
| Unicast Policy | 264 | 557 |

## Table size settings file

When you select **Adjust table sizes**, FortiConverter uses the maximum table sizes in the file **TargetPlatformTablesizeSetting.txt**, which is stored in the same folder as the FortiConverter executable file (for example, using the default installation path, **C:\Program Files (x86)\Fortinet\FortiConverter\TargetPlatformTablesizeSetting.txt**).

By default, the file contains the following values, which are suitable for high-end devices (for example, FortiGate 1200D or higher):

```
Address groups:20000
Addresses per group:1500
Custom service objects:4096
```

You can manually adjust these values by editing the file.

## Viewing maximum table sizes for your target device

On your target system, enter the following command:

```
print tablesize
```

The maximum table sizes are displayed in a response similar to the following output:

```
firewall addrgrp: 0 20000 20000
firewall addrgrp:member: 1500 0 0
firewall service custom: 0 4096 0
```

# NAT merge options

For Check Point and Cisco PIX conversions, you can select which types of NAT configuration FortiConverter uses to generate output firewall policies, or whether FortiConverter derives its NAT-based policies based on object names or object values.

Because it can take FortiConverter several hours to complete a conversion that includes a large number of NAT rules, Fortinet recommends that you turn off NAT merge for **all** types of NAT for your initial conversion. Then, after you resolve any issues with the conversion, run it again at a convenient time with NAT merge enabled.

## NAT merge depth

The FortiConverter NAT merge feature compares a firewall policy's source and destination address with addresses in NAT rules. When these addresses overlap, FortiConverter uses the NAT rules to generate additional policies in the output configuration.

If a policy has an address with a large range, it can overlap with many NAT rules, which generates many NAT policies. Because output that includes a large number of NAT policies can be hard to review, FortiConverter provides NAT merge depth options that can reduce the number of NAT policies.

The merge depth policies control both the type of NAT to merge and the scope of the merge:

- When you select **Off** for a type of NAT, FortiConverter does not perform NAT merge using NAT rules of that type. If it is turned off for all types, the output conversion contains the converted source configuration policies only.
- When you select **Object Names**, FortiConverter generates policies based on NAT rules only where the address name the rules use is found in a policy. For Cisco PIX, this option can also match NAT rules and policies if they contain addresses that match exactly.

  For example, a source configuration NAT rule dynamically translates the object "address1"(IP 10.10.10.10) to "200.200.200.200".

  The source configuration also has three polices:

  - policy1: source address is "address1"
  - policy2: source address is "10.10.10.0-10.10.10.255"
  - policy3: source address is "all"

  Only policy1 matches the NAT rule, because it shares the address object name, and policy2 and policy3 do not match because they do not reference the name "address1".

  Cisco PIX allows you to use an IP address to configure a NAT rule instead of a name. For example, the NAT rule 10.10.10.10 to 200.200.200.200. When **Object Names** is selected, this NAT rule matches a policy with source address 10.10.10.10, even though it does not refer to a object name because they have the exactly the same IP range. This is a useful option if you make use of supernet addresses that would match many address objects.
- When you select **Object Values**, FortiConverter generates policies based on NAT rules that have address values that fall anywhere in the range specified by a policy (overlap).

  For the example above, when **Object Values** is selected, the NAT rule that translates the object "address1"(IP 10.10.10.10) to "200.200.200.200" matches both policy2 and policy3.

**Object Values** generates the most accurate matching of NAT rules and policies, but in most cases, it also generates more NAT policies.

# New application features

## Folders

The new FortiConverter application allows you to create separate folders for your conversions.

**To add a folder**

1. Click the **New Folder** option from the menu on the left.
2. Enter a name for your new folder and press **OK**.
   Your new folder will appear in the menu on the left.

**To move conversions to a folder**

1. Select a conversion.
2. Click the **Change Folder** button, located at the bottom.
3. Select a folder for your conversion and press **OK**.


*High Performance Network Security*